SAP AG
Neurottstr. 16
D-69190 Walldorf

Security

Secure Network Communications

SNC User's Guide

Version 1.2, English
September 16, 1999

Copyright

SAP AG further does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP AG shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. The information in this documentation is subject to change without notice and does not represent a commitment on the part of SAP AG in the future.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT® and EXCEL® and SQL-Server® are registered trademarks of Microsoft Corporation.

IBM®, OS/2®, DB2/6000®, AIX®, OS/400® and AS/400® are a registered trademark of IBM Corporation.

OSF/Motif® is a registered trademark of Open Software Foundation.

ORACLE® is a registered trademark of ORACLE Corporation, California, USA.

INFORMIX®-OnLine *for SAP* is a registered trademark of Informix Software Incorporated.

UNIX® and X/Open® are registered trademarks of SCO Santa Cruz Operation.

ADABAS® is a registered trademark of Software AG.

SECUDE™ is a registered trademark of GMD-German National Research Center for Information Technology.

SAP®, R/2®, R/3®, RIVA®, ABAP/4®, SAPoffice®, SAPmail®, SAPaccess®, SAP-EDI®, SAP ArchiveLink®, SAP EarlyWatch®, SAP Business Workflow®, R/3 Retail® are registered trademarks of SAP AG.

SAP AG assumes no responsibility for errors or omissions in these materials.

Preface

This document is the user's guide for using Secure Network Communication (SNC) in SAP Systems. It is intended for system administrators and describes how to use SNC to protect your SAP System communications. The following list shows the contents of the *SNC User's Guide* in more detail:

- **Chapter 1** provides a brief introduction to SNC, including its advantages and the protection it provides.
- **Chapter 2** describes how SNC is built into the SAP System architecture, as a software layer with an interface to an external security product. It includes the requirements for external security products that you can use with SAP Systems. It also gives a general overview of the SAP System communication paths that can be protected with SNC and provides general comments and recommendations to consider when using SNC.
- **Chapter 3** describes how to activate SNC on your application servers and gateways. It explains the individual profile parameters and Customizing activities, as well as the steps you need to take for user maintenance.
- **Chapter 4** describes how to configure the individual SAP System components, to include SAPgui, external programs (RFC and CPIC), RFC and CPIC destinations, SAPlpd, SAProuter, and the SAP Internet Transaction Server. It also describes special cases and how to use SNC with C program interfaces.
- **Chapter 5** contains a list of the most Frequently Asked Questions (FAQs) pertaining to SNC.

- **Appendix A** shows a sample scenario using SNC.
- **Appendix B** lists the SNC-relevant tables in SAP Systems.
- **Appendix C** lists the various SNC maintenance tools provided with SAP Systems.
- **Appendix D** describes special cases in Releases 3.1G/H and 4.0A.
- **Appendix E** shows an example of SNC messages recorded in the work process logs or trace files when SNC is activated.
- **Appendix F** describes how to use SNC to protect SAPgui connections and RFC client programs under MAC™OS.
- **Appendix G** provides references to additional sources of information.

Style Conventions

This text format	helps you identify
Screen Text	words or characters you see on the screen (this includes system messages, field names, screen titles, menu names, and menu items).
`User Entry`	exact user input. These are words and characters you type on the keyboard exactly as they are in the documentation.
`<Variable User Entry>`	variable user input. Pointed brackets indicate that you replace these variables with appropriate keyboard entries.
ALL CAPITALS	report names, program names, transaction codes, table names, ABAP language elements, file names, and directories.
Book Title	cross-references to other books or references.
KEY name	keys on your keyboard. Most often, function keys (for example, F2 and the ENTER key) are represented this way.
`Technical Object Name`	names of technical objects outside of the SAP System (for example, UNIX or Windows NT file names or environment variables).

Icons in Text

Icon	Meaning
⚠	Caution
▶	Example
➡	Note
✓	Recommendation
💡	Tip

History of Changes

Version	Changes
1.2	We have improved formulations for establishing context throughout the guide. In addition, we have added the following information: • ***Chapter 1.3.1: Requirements*** Security products need to be certified by the SAP Complementary Software Program (CSP™). The certification process is now available. • ***Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*** In this chapter, we have added descriptions for the application server's profile parameters in Releases 3.1G/H/I and provide example SNC configurations for these releases. • ***Chapter 4.7: Communication Between the SAP Internet Transaction Server and SAP Systems*** In this chapter, we describe how to configure the SNC options to protect the communication between the SAP System and the Internet Transaction Server (ITS) components (available as of Release 4.5B). • ***Chapter 4.8.1: Using Microsoft's NT LAN Manager Security Support Provider for Single Sign-On under Windows NT*** In this chapter, we describe how to configure the system components for the Windows NTLMSSP Single Sign-On scenario. • ***Appendix G: References*** We include sources of additional information.
1.1	In Release 4.5, we introduce the profile parameter `snc/force_login_screen` on the SAP System application server. See *Chapter 3.7: SAP System Logon Screen.*
1.0	First version

Contents

1 INTRODUCTION 1-1

1.1 WHAT IS SNC? 1-1

1.2 WHAT DOES SNC DO? 1-2

2 SNC IN THE SAP SYSTEM ARCHITECTURE 2-1

2.1 TERMINOLOGY 2-1

2.2 THE SNC LAYER IN SAP SYSTEMS 2-4

2.2.1 Factors that Influenced the SNC Design 2-4

2.2.2 Integration of SNC and an External Security Product in the SAP System Architecture 2-5

2.3 EXTERNAL SECURITY PRODUCTS 2-6

2.3.1 Requirements 2-6

2.3.2 Naming Conventions 2-6

2.4 COMMUNICATION PATHS IN THE SAP SYSTEM ENVIRONMENT 2-8

2.5 GENERAL COMMENTS PERTAINING TO SNC PARAMETERIZATION 2-10

2.6 RECOMMENDATIONS 2-12

3 ACTIVATING SNC ON THE SAP SYSTEM APPLICATION SERVER 3-1

3.1 PREREQUISITES 3-1

3.2 PROFILE PARAMETER SETTINGS ON THE SAP SYSTEM APPLICATION SERVER 3-2

3.3 PROFILE PARAMETER SETTINGS ON THE GATEWAY 3-12

3.4 CUSTOMIZING IN THE SAP SYSTEM 3-14

3.4.1 Upgrade from 3.0/3.1 3-15

3.4.2 Access Control Lists (ACL) 3-15

3.4.2.1 User Access Control List 3-15

3.4.2.2 System Access Control List 3-15

3.4.3 Communication 3-16

3.4.3.1 Printing using SAPlpd 3-16

3.4.3.2 RFC Remote Function Call 3-16

3.4.3.3 CPIC 3-16

3.4.3.4 Maintain the External Security System 3-16

3.5 TRANSPORT THE CUSTOMIZING CONFIGURATION 3-17

3.5.1 Upgrade from 3.0/3.1 3-17

3.5.2 Access Control Lists 3-18

3.5.2.1 User Access Control List 3-18

3.5.3 System Access Control List 3-18

3.5.4 Communication ... 3-19

3.5.4.1 Printing using SAPlpd ... 3-19

3.5.4.2 RFC Remote Function Call ... 3-19

3.5.4.3 CPIC ... 3-19

3.6 USER MAINTENANCE IN THE SAP SYSTEM ... 3-20

3.6.1 Maintaining SNC Information for Dialog Users ... 3-20

3.6.2 Maintaining SNC Information for Non-Dialog Users ... 3-22

3.7 SAP SYSTEM LOGON SCREEN ... 3-25

4 CONFIGURING THE COMMUNICATION PARTNERS FOR USE WITH SNC ... 4-1

4.1 CONFIGURING SNC OPTIONS: SAPGUI → SAP SYSTEM ... 4-1

4.2 CONFIGURING SNC OPTIONS: EXTERNAL PROGRAMS → SAP SYSTEMS ... 4-7

4.2.1 External Programs → SAP Systems Using RFC ... 4-7

4.2.2 External Programs → SAP Systems Using CPIC ... 4-10

4.3 CONFIGURING SNC OPTIONS: USING RFC FROM SAP SYSTEMS ... 4-12

4.3.1 Maintaining RFC Destinations and their SNC Options Using Transaction SM59 ... 4-12

4.3.2 RFC: SAP System → R/2 ... 4-15

4.3.3 RFC: SAP System → SAP System ... 4-15

4.3.4 RFC: Internal Destinations ... 4-18

4.3.5 RFC: Logical Destinations ... 4-19

4.3.6 RFC: TCP/IP Connection - Start an External Program on an Application Server ... 4-19

4.3.7 RFC: TCP/IP Connection - Start an External Program on an Explicit Host ... 4-20

4.3.8 RFC: TCP/IP Connection - Start an External Program over SAPgui ... 4-22

4.3.9 RFC: TCP/IP Connection - Registered Program ... 4-23

4.3.10 Remote Logon Using Transaction SM51 ... 4-24

4.3.11 Remote Logon Using Transaction SM59 ... 4-25

4.3.12 Special Destinations ... 4-25

4.3.13 Destinations without RFCDES Entry ... 4-25

4.3.14 RFC Groups ... 4-25

4.4 CONFIGURING SNC OPTIONS: USING CPIC FROM SAP SYSTEMS ... 4-26

4.4.1 Maintaining CPIC Destinations and their SNC Options Using Transaction SM54 ... 4-26

4.4.2 CPIC: SAP System → R/2 Connection ... 4-29

4.4.3 CPIC: SAP System → SAP System ... 4-29

4.4.4 CPIC: Start an External Program over a Gateway ... 4-31

4.4.5 CPIC: Registered Program ... 4-32

4.5 CONFIGURING SNC OPTIONS: PRINTING ... 4-33

4.5.1 Printing on a Frontend Computer ... 4-33

4.5.2 Printing Using SAPlpd ... 4-33

4.6 CONFIGURING SNC OPTIONS: SAPROUTER ←→ SAPROUTER 4-39

4.7 CONFIGURING SNC OPTIONS: SAP INTERNET TRANSACTION SERVER → SAP SYSTEM........ 4-43

4.8 SPECIAL CASES 4-47

4.8.1 Using Microsoft's NT LAN Manager Security Support Provider for Single Sign-On under Windows NT 4-47

4.8.1.1 Installing the GSS-API V2........ 4-48

4.8.1.2 Activating SNC on the SAP System Application Server 4-48

4.8.1.3 Maintaining Users in the SAP System 4-49

4.8.1.4 Configuring SNC Options: SAPgui and SAP System 4-49

4.8.2 Communication with the Message Server 4-50

4.8.3 SAPgui Started per RFC........ 4-50

4.9 C PROGRAM INTERFACES 4-51

4.9.1 Interfaces to External CPIC Programs........ 4-51

4.9.2 Interfaces to External RFC Programs........ 4-52

5 FAQS 5-1

APPENDIX A SAMPLE SNC SCENARIO........ A-1

APPENDIX B SNC-RELATED TABLES A-3

APPENDIX C MAINTENANCE UTILITIES........ A-4

APPENDIX D SPECIAL CASES RELEVANT TO RELEASES 3.1G/H AND 4.0A A-4

D.1 Quality of Protection........A-4

APPENDIX E SNC MESSAGES A-5

APPENDIX F USING SNC WITH MAC™OS........ A-6

F.1 SAPgui........A-6

F.2 RFC Client Programs........A-6

APPENDIX G REFERENCES........ A-7

INDEX I-1

Figures

Figure 2-1: Integration of SNC and an External Security Product in SAP Systems 2-5

Figure 2-2: SAP System Communication Paths...2-8

Figure 2-3: Example of an SNC-Secured Network...2-13

Figure 3-1: SNC User Maintenance in the SAP System (Transaction SU01).................................3-21

Figure 3-2: SNC User Maintenance for Non-Dialog Users (SM30 – USRACLEXT) – Changing or Creating New Entries...3-23

Figure 3-3: Example Extended User ACL (Transaction SM30 – USRACLEXT).............................3-24

Figure 4-1: SAP Logon SNC Options (4.0B Front End) 4-4

Figure 4-2: Activating SNC for RFC Destinations...4-13

Figure 4-3: SNC Options for RFC Destinations..4-14

Figure 4-4: SNC Options for RFC Destinations: SAP System Connection with Load Balancing 4-16

Figure 4-5: Access Control List for SNC-protected RFCs from other SAP Systems 4-17

Figure 4-6: Maintaining SNC Options for CPIC Destinations (SM54) 4-27

Figure 4-7: Maintaining SNC Mode for CPIC Destinations..4-27

Figure 4-8: Maintaining SNC Options for CPIC Destinations 4-28

Figure 4-9: SNC Entries in the Access Control List for CPICs from SAP Systems.........................4-30

Figure 4-10: Spool Administration: Access Method Type S 4-34

Figure 4-11: Spool Administration: No Longer Ask for Print Requests in Host Spool........................4-35

Figure 4-12: Spool Administration: SNC Options 4-35

Figure 4-13: Spool Administration: Additional SNC Options 4-37

Figure 4-14: Spool Administration: Authorized Communication Partners for SAPlpd........................4-38

Figure 4-15: SNC Communication Between SAProuters..4-39

Tables

Table 2-1: SAP System Communication Paths....................2-9
Table 2-2: SNC Keywords for Parameterization 2-11
Table 3-1: SNC Profile Parameters by Release....................3-2
Table 4-1: SNC Command Line Parameters for SAPgui → SAP System 4-2
Table 4-2: SNC Parameters for RFC External Programs → SAP Systems....................4-8
Table 4-3: SNC Parameters for CPIC External Programs → SAP Systems....................4-10
Table 4-4: SNC Parameters for RFC from SAP Systems to Start a Registered Program....................4-23
Table 4-5: SNC Parameters for SAPlpd....................4-36
Table 4-6: SNC Parameters for the WGate 4-44
Table 4-7: SNC Parameters on the AGate for Communication with the WGate 4-44
Table 4-8: SNC Parameters on the AGate for Communication with the SAP System....................4-45
Table 4-9: Profile Parameter Settings for Single Sign-On Using Microsoft's NTLMSSP 4-48
Table 4-10: SNC-Relevant CPIC Functions....................4-51
Table 4-11: SNC-Relevant RFC Functions 4-52

Table A-1: SNC Tables Used for Incoming Connections A-3
Table A-2: SNC Tables Used for Outgoing Connections A-3
Table A-3: SNC-Relevant RFC Functions A-4

Tables

1 Introduction

In this chapter, we provide an introduction to Secure Network Communications (SNC), to include a short description of SNC, its advantages, and the protection it offers.

1.1 What is SNC?

SNC is a software layer in the SAP System architecture that provides an interface to an external security product.

SAP Systems include basic security measures, which include the SAP authorization concept and user authentication based on passwords. With SNC, you can extend SAP System security beyond these basic measures to include protection offered by an external security product.

Advantages of using SNC:

- SNC provides application-level, end-to-end security.

  SNC secures all communications between two SNC-protected components (for example, between SAPgui and an SAP System application server).
- You can implement additional security features that the SAP System does not directly provide (for example, Single Sign-On or the use of smart cards for authentication).
- You receive an individual approach. You use the security product of your choice, choosing the algorithms you want to use.
- You can change the security product at any time without affecting SAP System business applications.

1.2 *What does SNC do?*

SNC secures data communication paths.

SNC secures the data communication paths between the various SAP System components. There are well-known cryptographic algorithms that have been implemented by the external security products supported by SAP Systems. With SNC, you can apply these algorithms to your data for increased protection.

There are three levels of security protection you can apply. They are:

- Authentication only
- Integrity protection
- Privacy protection

Authentication only

When using the *Authentication only* protection level, the system verifies the identity of the communication partners. This is the minimum protection level offered by SNC.

No actual data protection is provided!

Integrity Protection

When using *Integrity protection*, the system detects any changes or manipulation of the data which may have occurred between the two end points of a communication.

Privacy Protection

When using *Privacy protection*, the system encrypts the messages being transferred to make eavesdropping useless. Privacy protection also includes integrity protection of the data. This is the maximum level of protection provided by SNC.

2 SNC in the SAP System Architecture

In this chapter, we provide an overview of SNC in the SAP System architecture. See the following sections:

- *Chapter 2.1: Terminology*
- *Chapter 2.2: The SNC Layer in SAP Systems*
  - *Chapter 2.2.1: Factors that Influenced the SNC Design*
  - *Chapter 2.2.2: Integration of SNC and an External Security Product in the SAP System Architecture*
- *Chapter 2.3: External Security Products*
  - *Chapter 2.3.1: Requirements*
  - *Chapter 2.3.2: Naming Conventions*
- *Chapter 2.4: Communication Paths in the SAP System Environment*
- *Chapter 2.5: General Comments Pertaining to SNC Parameterization*
- *Chapter 2.6: Recommendations*

2.1 Terminology

We use the following terms frequently when describing SNC:

- **Generic Security Services Application Programming Interface Version 2**
  (GSS-API V2)

  The GSS-API V2 is a standard interface to security functions that was developed by the Internet Engineering Task Force (IETF). SNC uses the GSS-API V2 as the standard interface for the function calls to external security products.

- **External security product's library**
  External library
  SNC_LIB
  gssapi library

  The terms, **external security product's library, external library, SNC_LIB**, or **gssapi library** refer to the library that contains the functions provided by the external security product. When the file name of the library is required for a component's configuration, we recommend you use a local copy of the library and include the complete path and file name in the reference.

- **Credentials**

  Credentials are user or component-specific information that allow the users or components to access their security information. The credentials may be located for example, in a protected file in the file system. They often have a limited life span. For example, a user's credentials may be created when the user logs on to a security product and deleted when he or she logs off.

- **External name**

  The external name is the identification that a user or other component (for example, an application server) has with the external security system. The external security product assigns and maintains the user's external name. For examples of external names, see *Chapter 2.3.2: Naming Conventions*.

- **SNC name**

  The SAP System refers not to the external name, but to an extended version of the external name, called the SNC name. You create the SNC name by providing a prefix with the external user name that designates the name type. As of Releases 3.1I and 4.0A, you can also use an optional `<product>` indicator in the prefix. See below for the SNC formats:

  - normal format: `<name type>:<external name>`
  - extended format: `<name type>/<product>:<external name>`

  Where:

  - `<name type>` indicates the name type syntax and may be one of the following values:

p	product-specific default printable name
s	host-based service name form
u	user name

    Defaults are product-specific. For example, SECUDE™ uses X.500 names by default. Kerberos uses Kerberos-principal names as default.

  - `<product>` indicates the security product used and can currently be one of the following values:

`krb5`	Kerberos
`secude`	SECUDE™
`sapntlm`	SAP-supplied indicator for the Windows NT LAN Manager Security Service Provider (NTLMSSP) on Win32 platforms (see *Chapter 4.8.1: Using Microsoft's NT LAN Manager Security Support Provider for Single Sign-On under Windows NT*).

    The `<product>` indicator is optional and available as of Releases 3.1I and 4.0A. If you omit it, the system uses the currently active product to determine the name syntax.

  - `<external name>` indicates the user's external name as it is known by the security product. (See the definition for external name.)

  When defining or referring to SNC names, make sure you include the name type prefix.

  Examples of SNC names:

  ```
  p:CN=miller, OU=ADMIN, O=SAP, C=DE
  p:miller@WDF.SAP-AG.DE
  s:sap00@hostxyz

  p/secude:CN=miller, OU=ADMIN, O=SAP, C=DE
  p/krb5:miller@WDF.SAP-AG.DE
  s/krb5:sap00@hostxyz
  ```

- **Canonical name**

  Because an X.500 name can have different forms that are all equivalent, the SAP System converts such names into a standard format, which we call the **canonical name**. (The SAP System uses a GSS-API V2 function for the conversion.)

- **Protection level**
  Quality of Protection (QoP)

  The protection level indicates what level of security should be applied to a communication (authentication only, integrity, or privacy).

- **SNC-protected communication**
  SNC protection

  SNC-protected communication or SNC protection refers to a communication between two components where all of the transferred information and data are protected using theSNC functions.

2.2 The SNC Layer in SAP Systems

In this section, we describe the factors that influenced the SNC design how SNC and an external security product are integrated into the SAP System architecture.

2.2.1 Factors that Influenced the SNC Design

Factors that influenced the design of SNC in SAP Systems include:

- **Existing restrictions**

  The following restrictions exist on cryptography use in software implementations:

  - **Import and export regulations**

    Certain countries enforce import or export regulations for software that uses cryptographic algorithms.

  - **Regulations on use**

    There may also be regulations restricting the use of such algorithms.

  - **Patents**

    Certain algorithms have been patented and are therefore protected from free distribution or use (at least for a limited period of time).

- **Customer requirements**

  Additionally, each customer has individual requirements for a "secure" environment. The following are a few examples of possible customer requirements:

  - Company-wide use of a security product to protect systems, including systems other than SAP Systems
  - Use of smart cards for authentication
  - Use of Single Sign-On

- **Goal: optimal solution over a standard interface**

  Our goal was to enable optimal security protection for each customer installation, taking into account the widely different local policies and interests. Additionally, each customer should be able to implement the security product of his or her choice.

  Therefore, the necessary security functions are integrated with SAP Systems using a standardized interface, namely the Generic Security Services Application Programming Interface Version 2 (GSS-API V2), which has been defined by the Internet Engineering Task Force (IETF).

2.2.2 Integration of SNC and an External Security Product in the SAP System Architecture

The SNC functions are integrated in the SAP System components (for example, the SAP System kernel, SAPgui, or RFC Library) as a layer between the SAP System kernel layer and the library provided by the external security product (See Figure 2-1).

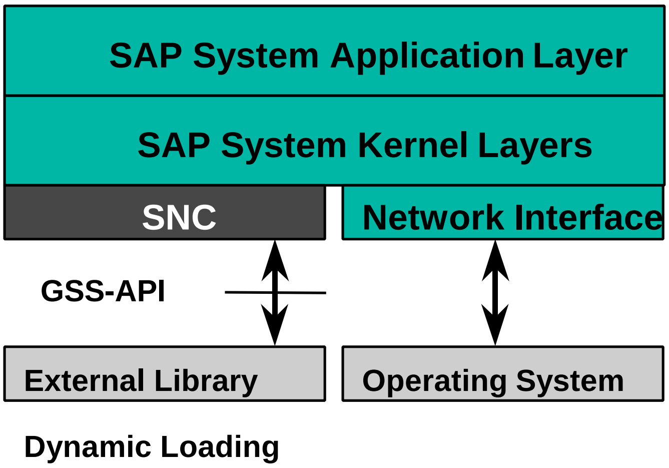


Figure 2-1: Integration of SNC and an External Security Product in SAP Systems

When SNC is initialized, the system dynamically loads the functions provided by the external library. Afterwards, when two components communicate using SNC, the SNC layer first processes the messages being sent and then sends them over the network using the SAP Network Interface. During this step, the SNC layer uses the functions provided by the external library to process the messages accordingly (for example, to apply encryption). The SNC layer accesses the external library using the GSS-API V2 interface. After processing the messages, the system sends them over the SAP Network Interface in the usual manner. Upon receipt, the SAP System component receiving the messages applies the corresponding external library functions in a similar manner, but reverses the process (for example, decryption).

All of the components involved in the communication need to use a library that implements the same GSS-API V2 functions. We cannot guarantee interoperability if different components use different security products with different implementations.

2.3 External Security Products

This chapter provides the requirements that SNC imposes on external security products and describes possible naming conventions that products may use.

2.3.1 Requirements

To use a security product with SAP Systems, the product must meet the following requirements:

- The product must provide the entire range of functions defined in the GSS-API V2 interface.
- The functions must be dynamically loadable.
- The product must be available on platforms supported by SAP Systems.
- The product must be certified for use by the SAP Complementary Software Program (CSP).

  The SAP CSP certifies external products for use with SAP Systems. For more information on product availability and certification, see the SAP CSP information in SAPNet [1] and SAPNet Note 66687 [9].

2.3.2 Naming Conventions

The various security products define their own naming conventions to assign their users' identifications. These external names are normally created independent of the user IDs in the SAP System. (You do need to define a relationship between the two IDs; we describe how to establish this relationship in *Chapter 3.6: User Maintenance in the SAP System.*)

In addition, to communicate using SNC, application servers and other SAP System services (which do not usually have user IDs in the SAP System) also need identifications for use with the security product. For successful authentication, the SAP System must also be able to recognize these external identifications.

This section describes a couple of the more popular naming conventions. For a more detailed description, see the documentation provided by the external security product.

The syntax of the external names is determined by the security product. However, in general, the entries are case-sensitive and blanks can neither be omitted nor their number increased.

Example 1:

This example shows an X.500 Distinguished Name. It is formed from different elements that represent a hierarchical name space.

```
CN=miller, OU=TEST01, O=SAP, C=DE
```

Where `CN` = Common Name, `OU` = Organizational Unit, `O` = Organization, and `C` = Country.

Example 2:

This example shows a Kerberos-principal name created from the user ID and domain (or realm).

```
miller@WDF.SAP-AG.DE
```

Recommendation: Use report RSUSR300 to create SNC names

In the following recommendation, we use an X.500 naming convention.

If possible, build the external name for a user from the SAP System user name and the rest as constants that are the same for all users. For example, for X.500 names, you can use the SAP System user ID for the `CN` element (`CN` = `miller` in Example 1), and for the other elements (`OU, O, C`), use constant values that are the same for all users.

The same applies to the external name for SAP System components such as the application server. Build the external name from a server-specific component and the rest as constant components. For the server-specific component, we recommend the following syntax:

```
sap<system number>.<server name>
```

For example, the SAP System application server on the server `hs0017` where the system number is 01 has the external name:

```
CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE
```

If you define such a naming convention, you can use the report RSUSR300 to automatically generate the users' and components' SNC names in the SAP System.

2.4 Communication Paths in the SAP System Environment

In this section, we provide an overview of the communication paths you can protect with SNC (see Figure 2-2).

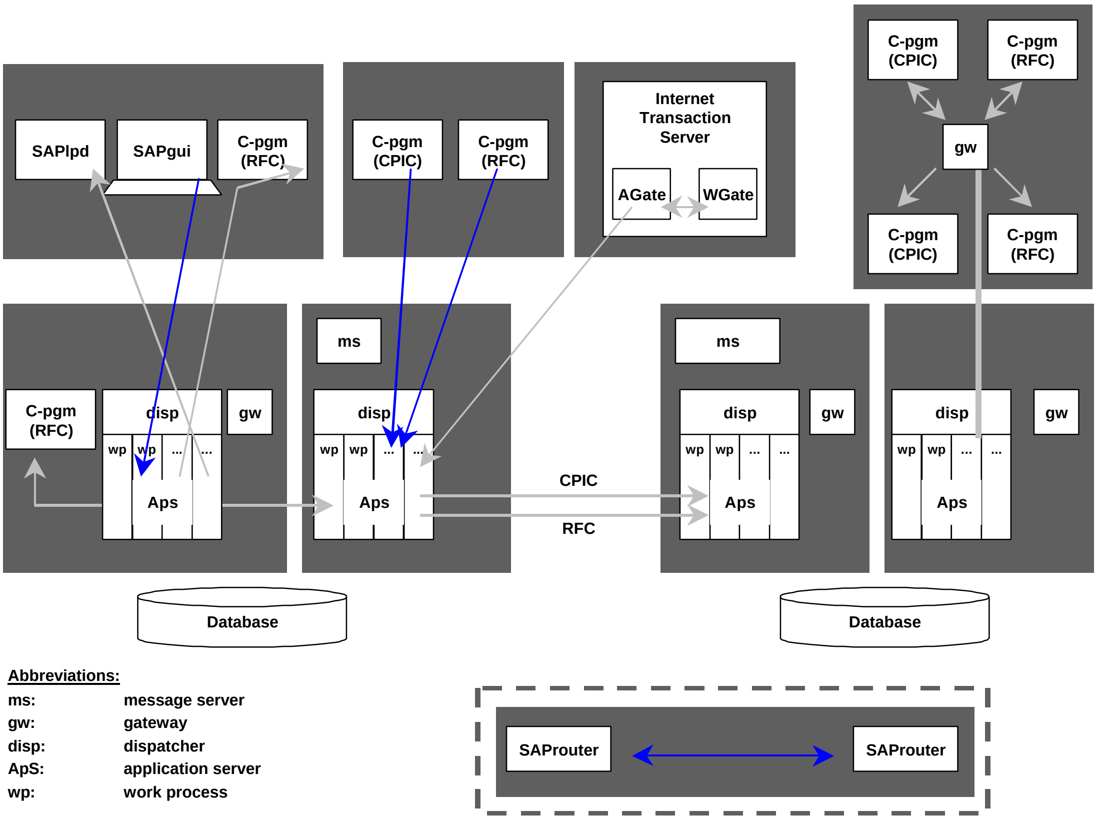


Figure 2-2: SAP System Communication Paths

The following system components are involved in the SAP System communication schema:

- SAP System application server
- SAPgui
- SAPlpd
- External RFC programs
- External CPIC programs
- SAProuter
- SAP Internet Transaction Server

The following communication paths result:

Table 2-1: SAP System Communication Paths

From		To	Using	SNC-Protection as of Version	See Chapter
SAPgui	→	SAP System		3.1G	4.1
Ext. Program	→	SAP System	RFC	4.0A	4.2.1
Ext. Program	→	SAP System	CPIC	4.0A	4.2.2
SAP System	→	SAP System	RFC	4.0A	4.3
SAP System	→	SAP System	CPIC	4.0A	4.4
SAP System	→	Ext. RFC program	RFC	4.0A	4.3.6 - 4.3.9
SAP System	→	Ext. CPIC program	CPIC	4.0A	4.4.4 - 4.4.5
SAP System	→	SAPlpd		3.1G	4.5
SAProuter	→	SAProuter		4.0A (SAProuter Version 30)	4.6
ITS	→	SAP System		4.5B	4.7

For information about how to establish SNC protection for these connections, see *Chapter 4: Configuring the Communication Partners for Use with SNC.*

2.5 General Comments Pertaining to SNC Parameterization

SNC protects the logical link between the end points of a communication. The link is initiated from one side (the initiator) and accepted by the other side (the acceptor). For example, when a SAPgui starts a dialog with the SAP System, the SAPgui is the initiator of the communication and the application server is the acceptor.

Both sides of the communication link need to specify SNC options.

The initiator must specify:

- Whether the communication should use SNC protection
- The SNC name of the communication partner (the target name)
- The location of its own external library
- The data protection level to apply

The acceptor must specify:

- Whether or not it should only accept SNC-protected communications
- Its own SNC name
- The location of its own external library
- The data protection levels to accept

Depending on the communication partners and types of communication you want to apply, you need to configure the settings in various places in the SAP System environment. You define the configuration either in the profile parameters, in initializing files, or by using the appropriate maintenance transactions. *Chapter 3: Activating SNC on the SAP System Application Server* and *Chapter 4: Configuring the Communication Partners for Use with SNC* explain in detail the steps you need to take to activate and configure each of the communication partners.

Before proceeding, you should be familiar with the following key words:

Table 2-2: SNC Keywords for Parameterization

Keyword	Description	Value
`SNC_MODE`	SNC activation indicator	0 : Do not apply SNC to connections 1 : Apply SNC to connections
`SNC_MYNAME`	Initiator's SNC name	`<own_snc_name>`
`SNC_PARTNERNAME`	Communication partner's SNC name	`<partner_snc_name>`
`SNC_QOP`	Quality of Protection (Security Level)	1 : Apply authentication only 2 : Apply integrity protection (authentication) 3 : Apply privacy protection (integrity and authentication) 8 : Apply the default protection 9 : Apply the maximum protection
`SNC_LIB`	external security product's library	Path and file name of the library

The SNC Quality of Protection, (SNC_QOP, QoP) indicates the level of protection to apply to a communication path. Some external security products do not support all levels of protection. If you request a quality of protection level that is higher than that which is supported by your security product, then the system uses the highest available protection level of your product instead.

2.6 Recommendations

We recommend you consider the following points before proceeding with the SNC configuration:

- You cannot use SNC to protect the communication path between the SAP System application server and the database.

  When communicating with the database, the communication end points are located within the database modules and not in the SAP System modules. Therefore, you cannot use SNC to protect this communication path. We recommend you isolate the (sub-)network that contains your database from the rest of your network and protect it with a firewall (see Figure 2-3).

- To save on performance, protect internal remote function calls (RFCs) using the network infrastructure instead of SNC.

  Time critical communications often occur between application servers within the SAP System (for example, RFCs). To save on performance (establishing an SNC-protected connection is time consuming), we recommend you protect these communications by establishing a secure sub-network. Within this sub-network, you can securely operate without needing to use SNC (see Figure 2-3). See also the description for the profile parameter `snc/r3int_rfc_secure` on page 3-7. (Set it to the value "0". Internal RFCs are then not protected with SNC.)

- You need to allow access to end users beyond the secure (sub-)network.

  The connection to the SAP System over SAPgui must be available to every end point and for every end user. These connection requests must be able to cross the firewall.You either have to open the SAP System dispatcher port directly on the firewall (`sapdp<nn>`), or route the connection request over a SAProuter. The default SAProuter port is 3299.

  > You can configure your system so that only SNC-protected SAPgui connections are accepted. Specify this configuration in the profile parameters and in the user master records. You can set this option to apply to all SAPgui connections or for specific users only. For more information, see the profile parameter `snc/accept_insecure_gui` on page 3-9.

- Use the "secure" gateway port (`sapgw<nn>s`) to allow only SNC-protected connections between the SAP System and external RFC server programs.

  The connection to the SAP System must also be available for external RFC server programs. When using SNC, we recommend you only allow SNC-protected connections between SAP Systems and the external RFC server programs. To enforce SNC protection, configure your firewall to only accept requests to the "secure" gateway port (`sapgw<nn>s`) and deny requests to the "normal" gateway port (`sapgw<nn>`). The gateway denies any incoming requests over the secure port that are not SNC-protected.

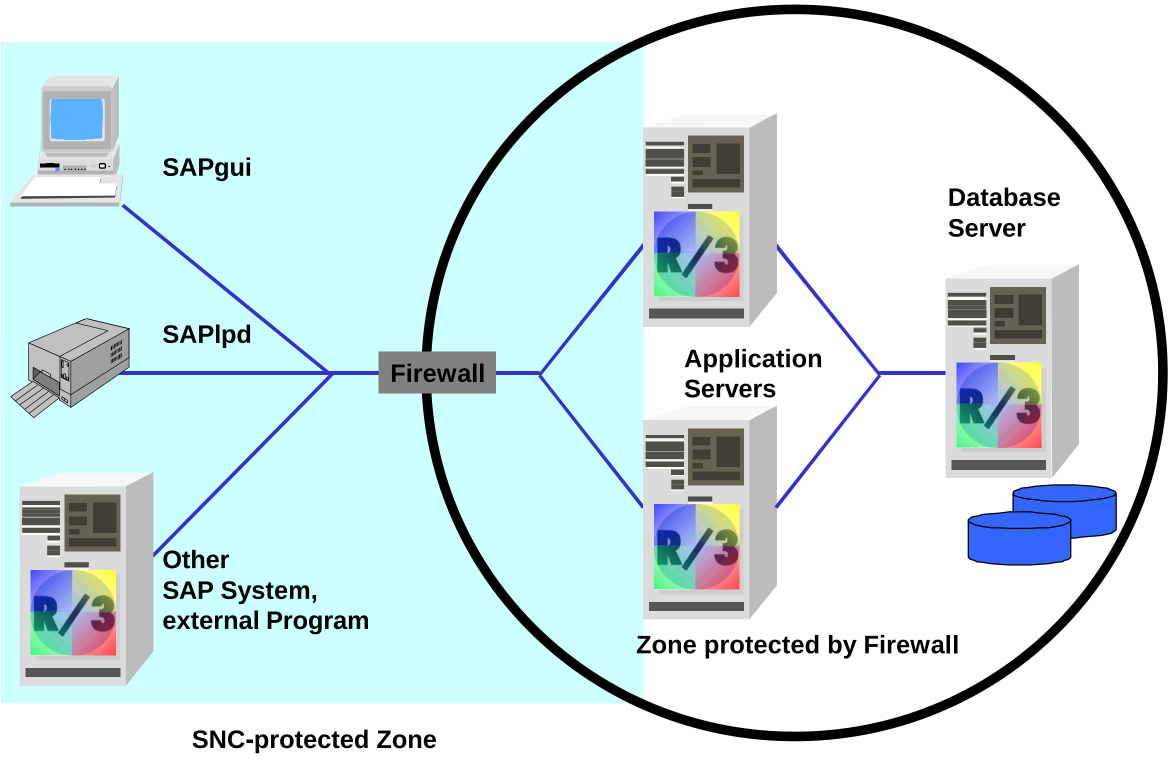


Figure 2-3: Example of an SNC-Secured Network

The following ports are the secure gateway ports that must be accessible through the firewall:

- `sapgw<nn>s/tcp` 4800-4899

  where <nn> is the SAP System number

As an alternative, you can allow access to the ports over a SAProuter. In this case, you need to configure your firewall to deny all requests to other ports and only accept requests to the SAProuter port. You then need to make the necessary entries in the SAProuter's route permission table, where the SAProuter specifies to which secured port on which gateway (`sapgw<nn>s`) access is allowed. For more information, see *Chapter 4.6: Configuring SNC Options: SAProuter ←→ SAProuter*.

3 Activating SNC on the SAP System Application Server

In this chapter, we describe how to activate SNC on the SAP System application server. See the following sections:

- *Chapter 3.1: Prerequisites*
- *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*
- *Chapter 3.3: Profile Parameter Settings on the Gateway*
- *Chapter 3.4: Customizing in the SAP System*
- *Chapter 3.5: Transport the Customizing Configuration*
- *Chapter 3.6: User Maintenance in the SAP System*
- *Chapter 3.7: SAP System Logon Screen*

3.1 Prerequisites

- **External security product**
  - The external security product must be installed on your application servers.

    Note the following information from the external security product's installation. You need it for the configuration on the SAP System application servers. See the documentation provided by the external security product vendor if necessary.

    - External names of the participants

      You need to know the users' IDs as they are known to the external security product, as well as the external names of the application servers and other system components.

    - Paths and file names where the external libraries are located
  - You may also need to perform certain activities to establish a secure environment for your application servers or other system components. These activities depend primarily on the security product you use. Make sure you are aware of such procedures and have accomplished them before proceeding with the profile settings on the application server. For example, you may need to log on to the security product or make certain entries in a local server table. For details, see the documentation provided by the security product vendor.
- **Homogeneous configuration on all application servers**

  We recommend you configure all of your SAP System application servers the same way, with the exception of the server-specific SNC name and the platform-specific library name.

  In addition, do not create SAP Logon groups that contain bothSNC-enabled application servers and non-SNC servers! Although it is possible to run SNC servers with non-SNC servers within a complete SAP System, mixing SNC and non-SNC servers in a single logon group will produce errors in the load-balancing modules.
- **Implementation in phases**

  It may not be feasible to establish SNC system-wide in a single step and you may want to introduce it into sub-systems in phases. You can successfully implement SNC in phases by modifying the profile parameters accordingly. For example, you can allow non-protected connections parallel to protected connections.

In the following section, we discuss the profile parameters on the SAP System application server. These settings provide the framework necessary to operate the SAP System under SNC protection. For the individual communication settings, for example, between SAPgui and the application server, you have to decide what level of protection you need and set the corresponding parameters accordingly. We describe the steps to take for each of the individual communication partners in *Chapter 4: Configuring the Communication Partners for Use with SNC.*

We also provide an overview showing the scenario that we use in our examples in *Appendix A: Sample SNC Scenario*.

3.2 Profile Parameter Settings on the SAP System Application Server

Use transaction RZ10 to maintain the profile parameters.

Set the profile parameters in the application server instance profile. Note that the parameter `snc/identity/as` is instance-specific; the parameter `snc/gssapi_lib` is platform-specific.

Table 3-1: SNC Profile Parameters by Release

Profile Parameter	3.IG/H/I	4.0A/B	4.5 and higher
`snc/enable`	X	X	X
`snc/user_maint`	X		
`snc/gssapi_lib`	X	X	X
`snc/identity/as`	X	X	X
`snc/data_protection/max`	X	X	X
`snc/data_protection/min`	X	X	X
`snc/data_protection/use`	X	X	X
`snc/r3int_rfc_secure`		X	X
`snc/r3int_rfc_qop`		X	X
`snc/permit_insecure_comm` (must be set to the value "1")	X		
`snc/accept_insecure_cpic`		X	X
`snc/permit_insecure_gui`	X		
`snc/accept_insecure_gui`		X	X
`snc/accept_insecure_r3int_rfc`		X	X
`snc/accept_insecure_rfc`		X	X
`snc/permit_insecure_start`		X	X
`snc/force_login_screen`			X

We describe the parameters in more detail below.

snc/enable

Short description: Activate SNC on the application server

Valid Releases: All

Description: Set this parameter to the value "1" to activate SNC on the application server. The system then executes the SNC initialization at start-up.

Strategy:

As default, once you have activated SNC (`snc/enable` = 1), the system only accepts SNC-protected connections. If your SAP System is isolated by means of packet-filtering routers and you want to accept conventional connections that are not protected with SNC parallel to SNC-protected connections, then you must also set the appropriate parameters (see `snc/accept_insecure_gui`, `snc/accept_insecure_rfc`, `snc/accept_insecure_cpic`).

The SNC modules require the path and file name of the security product's shared library (for example, `snc/gssapi_lib` = `/usr/local/lib/libsecude.so`). If you have activated SNC , then the system loads this library at runtime. If the system cannot find or open the file, then an error message occurs and the process terminates.

(The error message comes from the module SncInit() and is called SNCERR_INIT.)

Default value: 0 (SNC is not activated)

Affected parameters:

`snc/gssapi_lib` (path and file name of the external shared library)
`snc/identity/as` (SNC name of the application server as known by the external security product)
`snc/accept_insecure_gui` (accept unprotected SAPgui logons)
`snc/accept_insecure_rfc` (accept unprotected RFCs)
`snc/accept_insecure_cpic` (accept unprotected CPICs)
`snc/data_protection/min` (minimum requirement on the protection level)
`snc/data_protection/max` (maximum level of protection for connections initiated by the SAP System)
`snc/data_protection/use` (recommended level of protection)
`snc/r3int_rfc_secure` (starting internal RFCs with SNC)
`snc/rfc_qop` (protection level for internal RFCs)
`snc/permit_insecure_start` (allows the gateway to programs without using SNC-protected communications)

Valid entries, formats:

0 : SNC is disabled
1 : SNC is activated

snc/user_maint

Short description: Transaction SU01: Maintenance of SNC name

Valid Releases: Release 3.1 only

Description: Set this parameter to receive an additional field in the user maintenance transaction SU01 for maintaining SNC names. (See *Chapter 2.3.2: Naming Conventions* for information on SNC names.)

Default value: 0 (no *SNC name* field)

Affected parameters: None

Valid entries, formats:

0 : There is no *SNC name* field included in user maintenance
1 : The *SNC name* field is included in user maintenance

snc/gssapi_lib

Short description: Path and file name of the GSS-API V2 shared library.

Valid Releases: All

Description: This parameter contains the path and file name of the GSS-API V2 shared library. The path and file name are determined by the security product and are established when the security product is installed.

Once SNC has been activated (`snc/enable` = 1), this library will be loaded at runtime. If the system cannot find or open this file, then the process terminates with an error.

The naming convention for the file name, its extension, and any dynamic references to other shared objects or libraries depends on the operating system you use.

UNIX Platforms:

If the shared library contains dynamic references to other shared libraries or objects, then you may have to set the search path for the dynamic loader in the environment parameters before the library can be properly loaded. The corresponding environment variables for the various UNIX platforms are indicated below:

- `LD_LIBRARY_PATH` (Solaris, Sinix, OSF/1, Reliant UNIX, Digital UNIX)
- `SHLIB_PATH` (HP-UX)
- `LIBPATH` (AIX)

Default value: The default value is platform-specific and, in general, no library actually exists with the supplied default name. You need to set this parameter appropriately for your security product.

Affected parameters: None

Valid entries, formats: File name up to 255 characters long
(We recommend including the complete path and file name.)

`snc/identity/as`

Short description: SNC name of the application server

Valid Releases: All

Description: This parameter contains the name type and name of the application server as it is known by the external security product. The application server specifies this name when requesting its accepting credentials or to initiate security contexts. The system also distributes this name over the message server as the target SNC name for SAP Logon groups and for load-balancing RFCs.

Format: `<name type>:<external name>` or
`<name type>/<product>:<external name>`

Where:

`<name type>`: The type is specified by a prefix.

`<product>`: The product name is an optional parameter supported as of Releases 3.1I and 4.0.

`<external name>`: The format of the external name is supplied by the security product vendor (for example, an X.500 name). The assigning of the name also occurs in an external process.

Examples:

```
p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE
p:sap01/hs0017@WDF.SAP-AG.DE
p:XY_DOMAIN\C11adm
```

Default value: None

Valid entries, formats: See *Chapter 2.1: Terminology* and *Chapter 2.3.2: Naming Conventions..*

`snc/data_protection/max`

Short description: Maximum level of data protection for connections initiated by the SAP System

Valid Releases: All

Description: Release 3.1G/H:

In these releases, this parameter specifies the maximum protection level that the application server accepts. If a client uses a higher protection level, the connection is aborted.

Release 3.1I:

Release 3.1I does not use this parameter.

Release 4.0A:

In Release 4.0A, this parameter also specifies the maximum protection level for incoming connections to the application server. For outgoing connections, it specifies the maximum level of protection to apply to the data. If a higher value is encountered, for example, in anRFC destination's profile, then the connection is terminated with an error.

`snc/data_protection/max` (continued)

Description (continued):

as of Release 4.0B:

As of Release 4.0B, this parameter specifies the level of protection for connections that are initiated from the SAP System and where the quality of protection level for the CPIC or RFC destination is set in the SNC options to use the maximum level of protection (QoP = 9).

As of Release 4.0B, this parameter does not specify a maximum limit on the protection level for incoming or outgoing connections!

Note: We recommend you keep the default setting for this parameter in Releases 3.1 and 4.0A.

Note: For more information about the QoP in Releases 3.1 and 4.0A, see *Appendix D: Special Cases Relevant to Releases 3.1G/H and 4.0A.*

Default value: 3 (privacy)

Affected parameters:

`snc/enable` (activate SNC)
`snc/data_protection/min` (minimum requirement on protection level)
`snc/data_protection/use` (recommended level of protection)

Valid entries, formats:

`>= snc/data_protection/use`
1 : Secure authentication only
2 : Data integrity protection
3 : Data privacy protection

`snc/data_protection/min`

Short description: Minimum data protection level required for SNC communications

Valid Releases: All

Description: This parameter specifies the lowest level of protection to accept when transferring data. The SNC layer negotiates with the communication partner to try and apply at least this level of protection to incoming data. If the specified protection level is not possible, an error occurs and the transfer is terminated.

Default value: 2 (integrity)

Affected parameters:

`snc/enable` (activate SNC)
`snc/data_protection/max` (maximum protection level for connections initiated by the SAP System)
`snc/data_protection/use` (recommended level of protection)

Valid entries, formats:

`<= snc/data_protection/use`
1 : Secure authentication only
2 : Data integrity protection
3 : Data privacy protection

`snc/data_protection/use`

Short description: Default level of data protection for connections initiated by the SAP System

Valid Releases: All

Description: This parameter applies to CPIC and RFC connections only. It specifies the level of protection for CPIC or RFC connections that are initiated from the SAP System and where the quality of protection level for the destination is set in the SNC options to use the default level of protection (QoP = 8).

Default value: 3 (privacy)

Affected parameters:
`snc/enable` (activate SNC)
`snc/data_protection/min` (minimum requirement on protection level)
`snc/data_protection/max` (maximum protection level for connections initiated by the SAP System)

Valid entries, formats:
`<= snc/data_protection/max`
`>= snc/data_protection/min`
1 : Secure authentication only
2 : Data integrity protection
3 : Data privacy protection
9 : Use the value from `snc/data_protection/max`

`snc/r3int_rfc_secure`

Short description: Use SNC for initiating internal RFC communications.

Valid Releases: As of Release 4.0

Description: This parameter specifies whether RFCs to internal destinations within the same SAP System should be protected with SNC.

Due to possible effects on performance, you should carefully consider the necessity of securing RFCs to internal destinations with SNC. You can achieve a comparable level of security for internal destinations with an adequate network infrastructure (see *Chapter 2.6: Recommendations*).

Default value: 0 (internal RFC connections are not SNC-protected)

Affected parameters:
`snc/enable` (activate SNC)
`snc/accept_insecure_rfc` (accept unprotected RFCs)
`snc/accept_insecure_r3int_rfc` (accept unprotected internal RFCs)

Valid entries, formats:
0 : Internal RFCs are unprotected
1 : Internal RFCs are protected with SNC

snc/r3int_rfc_qop

Short description: Quality of protection for internal RFCs that use SNC protection.

Valid Releases: As of Release 4.0

Description: This parameter specifies the protection level (Quality of Protection, QoP) to apply to internal RFCs, as long as SNC for internal RFCs is enabled (`snc/r3int_rfc_secure` = 1).

Default value: 8 (use the value from `snc/data_protection/use`)

Affected parameters:
`snc/enable` (activate SNC)
`snc/r3int_rfc_secure` (use SNC-protection for internal RFCs)

Valid entries, formats:
`>= snc/data_protection/min`
1 : Secure authentication only
2 : Data integrity protection
3 : Data privacy protection
8 : Use the value from `snc/data_protection/use`
9 : Use the value from `snc/data_protection/max`

snc/permit_insecure_comm

Short description: Permit insecure CPIC communication to an SNC-enabled application server

Valid Releases: Release 3.1

Description: As default, once SNC has been activated (`snc/enable` = 1), the SAP System application server rejects all CPIC connections that are not protected with SNC.

Because Release 3.1 does not support SNC-protected CPIC connections, you need to set this parameter to the value "1" to allow unprotected CPIC connections.

Default value: 0 (only secure connections are permitted)

Affected parameters: `snc/enable` (activate SNC)

Valid entries, formats:
0 : Insecure connections are not permitted
1 : Insecure connections are permitted

`snc/accept_insecure_cpic`

Short description: Accept unprotected incoming CPIC connections on an SNC-enabled application server.

Valid Releases: As of Release 4.0

Description: As default, once SNC has been activated (`snc/enable` = 1), the SAP System application server rejects all incoming CPIC connections from external C programs or other SAP Systems that are not protected with SNC.

Set this parameter (see *Valid entries, formats*) to override the default configuration and accept unprotected connections (for example, connections from existing CPIC programs, or from SAP Systems that are not protected with SNC).

Default value: 0 (only SNC-protected connections are allowed)

Affected parameters: `snc/enable` (activate SNC)

Valid entries, formats:

0 : Reject unprotected connections
1 : Accept unprotected connections
U: Accept unprotected connections for those users who have the appropriate flag set in their user master record (see *Chapter 3.6: User Maintenance in the SAP System*)

`snc/permit_insecure_gui`

Short description: Accept logon attempts coming from SAPgui that are not protected with SNC on an SNC-enabled application server.

Valid Releases: Release 3.1 only (The parameter `snc/accept_insecure_gui` replaces this parameter in Release 4.0.)

Description: As default, once SNC has been activated (`snc/enable` = 1), the SAP System application server rejects all SAPgui connection requests that are not protected with SNC.

Set this parameter (see *Valid entries, formats*) to override the default configuration and accept unprotected logon requests (for example, connections from an older SAPgui that cannot use SNC protection).

If you allow unprotected logon requests, then the SAPgui configuration determines whether or not a user's logon uses SNC protection.

Default value: 0 (only SNC-protected logons are allowed)

Affected parameters: `snc/enable` (activate SNC)

Valid entries, formats:

0 : Reject unprotected logons
1 : Accept unprotected logons

`snc/accept_insecure_gui`

Short description:	Accept logon attempts coming from SAPgui that are not protected with SNC on an SNC-enabled application server
Valid Releases:	As of Release 4.0
Description:	See the description for `snc/permit_insecure_gui`.
Default value:	0 (only SNC-protected logons are allowed)
Affected parameters:	`snc/enable` (activate SNC)
Valid entries, formats:	0 : Reject unprotected logons 1 : Accept unprotected logons U: Accept unprotected logons for only those users who have the appropriate flag set in their user master record (see *Chapter 3.6: User Maintenance in the SAP System*)

`snc/accept_insecure_r3int_rfc`

Short description:	Accept unprotected internal RFC-connections on an SNC-enabled application server
Valid Releases:	as of Release 4.0
Description:	Set this parameter to accept unprotected RFC connections that originate from internal SAP Systems and have internal destinations (see transaction SM59), even if you generally require SNC protection for RFC connections (`snc/accept_insecure_rfc` = 0). **Note:** This parameter is effective only if `snc/accept_insecure_rfc` = 0. Otherwise, the system accepts all RFC connections, both internal and external, regardless of this parameter's setting.
Default value:	1 (accept unprotected internal RFC connections)
Affected parameters:	`snc/enable` (activate SNC) `snc/accept_insecure_rfc` (accept unprotected RFCs) `snc/r3int_rfc_secure` (starting internal RFCs with SNC)
Valid entries, formats:	0 : Reject unprotected internal RFCs 1 : Accept unprotected internal RFCs

snc/accept_insecure_rfc

Short description: Accept unprotected incoming RFC-connections on an SNC-enabled application server

Valid Releases: As of Release 4.0

Description: As default, once SNC has been activated (`snc/enable` = 1), the SAP System application server rejects all incoming RFC connections from external C programs or other SAP Systems that are not protected with SNC.

Set this parameter (see *Valid entries, formats*) to override the default configuration and accept unprotected RFC connections (for example, connections from older RFC programs or SAP Systems that are not protected with SNC).

This parameter can apply to all RFC connections (internal and external), or to external RFC connections only (see *Valid entries, formats* below). The parameter `snc/accept_insecure_r3int_rfc` applies specifically to internal RFCs.

Default value: 0 (reject unprotected RFC connections)

Affected parameters: `snc/enable` (activate SNC)
`snc/accept_insecure_r3int_rfc` (accept unprotected internal RFCs)

Valid entries, formats:

0 : Reject unprotected external RFCs (internal RFCs are either accepted or rejected depending on the parameter `snc/accept_insecure_r3int_rfc`)
1 : Accept all unprotected RFCs (internal and external)
U: Accept unprotected external RFCs for those users who have the appropriate flag set in their user master record (see *Chapter 3.6: User Maintenance in the SAP System*)

snc/permit_insecure_start

Short description: Permit the starting of programs without using SNC-protected communications, even when SNC is enabled.

Valid Releases: As of Release 4.0

Description: As default, once SNC has been activated (`snc/enable` = 1), the gateway refuses to start programs when the communications are not SNC-protected.

Set this parameter (see *Valid entries, formats*) to override the default configuration and allow the gateway to start programs using unprotected communications.

Default value: 0 (start programs only with SNC-protected communication)

Affected parameters: `snc/enable` (activate SNC)

Valid entries, formats:

0 : Start programs only with SNC-protected communication
1 : Start programs without SNC-protected communication

snc/force_login_screen

Short description: Display logon screen for each SNC-protected logon

Valid Releases: As of Release 4.5

Description: If you set this parameter to the value "1", the system displays the logon screen for every logon, even if the communication is secured with SNC.

Otherwise, if the system can uniquely map the SNC or external name from the logon request to a single user in the SAP System, then it does not display the logon screen. (The SAP System user with the given SNC or external name must exist in the SAP System once and in only one client.)

Default value: 0 (the logon screen is only displayed if necessary)

Affected parameters: `snc/enable` (activate SNC)

Valid entries, formats:
0 : The logon screen is displayed only when necessary
1 : The logon screen is always displayed

The following examples show the profile parameter settings for a SAP System application server.

Release 3.1:

```
snc/enable = 1
snc/user_maint = 1
snc/data_protection/min = 2
snc/data_protection/max = 3
snc/data_protection/use = 3
snc/permit_insecure_comm = 1
snc/permit_insecure_gui = 0
snc/gssapi_lib = /usr/local/secude/lib/libsecude.sl
snc/identity/as = p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE
```

Release 4.0:

```
snc/enable = 1
snc/data_protection/min = 2
snc/data_protection/max = 3
snc/data_protection/use = 3
snc/accept_insecure_gui = 0
snc/accept_insecure_cpic= 0
snc/accept_insecure_rfc = 0
snc/accept_insecure_r3int_rfc = 1
snc/r3int_rfc_secure = 0
snc/r3int_rfc_qop    = 3
snc/permit_insecure_start = 1
snc/gssapi_lib = /usr/local/secude/lib/libsecude.sl
snc/identity/as = p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE
```

The parameters `snc/gssapi_lib` and `snc/identity/as` are specific to the application server.

3.3 Profile Parameter Settings on the Gateway

To use SNC for securing connections that connect via the SAP gateway, you also need to set the appropriate parameters in the gateway profile. The gateway itself does not directly use the routines from the security product; however, it does supply the SNC configuration parameters to the programs that it starts.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. In Release 3.1, you need to set the profile parameter `snc/permit_insecure_comm` to the value "1". The rest of the description in this section applies only as of Release 4.0.

The following profile parameters are relevant for the gateway settings:

- **`snc/enable`**

  For a gateway to accept SNC-protected connections, you need to set the profile parameter `snc/enable` to the value "1". The gateway then knows that an SNC environment is in operation and takes the following precautions:

  - In addition to the standard port (`sapgw<nn>`), it opens a "secured" port (`sapgw<nn>s`), where it accepts only connections that use SNC protection.
  - It starts programs only when SNC protection for the communication is used. You may explicitly allow the starting of programs without using SNC protection by setting the parameter `snc/permit_insecure_start` (see the description below).

- **`snc/gssapi_lib`**

  As with the application server, if `snc/enable` = 1, then the parameter `snc/gssapi_lib` must contain the path and file name of the external library. The gateway passes this information to the external programs that it starts.

- **`snc/permit_insecure_start` (`snc/permit_insecure_comm` in Release 3.1)**

  If `snc/enable` = 1, then the gateway does not start or register any external programs without using SNC-protected communications (as default). You can explicitly override this configuration by setting the parameter `snc/permit_insecure_start` to the value "1". The gateway will then start or register programs even if SNC protection is not used for the communication. The parameter is only necessary if programs without SNC protection are to be directly started by or registered on the gateway.

  If the gateway is started directly on an application server, it uses the application server's profile settings. In this case, the parameters `snc/enable` and `snc/gssapi_lib` are set in the application server's profile. For the gateway, you then only need to consider the parameter `snc/permit_insecure_start` (or `snc/permit_insecure_comm`).

  If a gateway is to be started independent of the SAP System application server ("Stand Alone Gateway"), then you need to consider all of the above mentioned parameters.

Because the gateway passes the name of the external library on to the programs that it starts, as well as for security reasons, you should **only start programs on the computer where the gateway is located.** To prevent remote program starts, include the following parameter settings in the gateway profile:

- **As of Release 4.5A:**

  ```
  gw/rem_start=DISABLED
  ```

- **Releases 4.0A and 4.0B:** (In these releases, you need to define an invalid remote shell to prevent remote program starts.)

  ```
  gw/rem_start=REMOTE_SHELL
  gw/remsh=.
  ```

  The gateway uses the common Berkeley remote shell (`rsh` or `remsh`) to start programs on remote hosts. The Berkeley remote shell performs only a simple authentication based on the IP address and cannot protect the TCP datastream that it uses. Therefore, we recommend you do not use the starting of programs on remote hosts when using SNC.

3.4 Customizing in the SAP System

As of Release 4.0, the SNC administration activities are included in Customizing. To access the SNC activities in Customizing, choose *Basis Components* → *System Administration* → *Management of External Security Systems* → *Secure Network Communication*. You can also access the structure with transaction SO70; the structure is SIMG_BCSNC.

Because the system needs to convert the SNC name into canonical form, which uses an SNC function, you should activate SNC on the application server before proceeding with the Customizing activities. However, as an alternative, you can continue without activating SNC and perform *Check canonical SNC names* as the last activity. The individual activities are listed below and described in the following sections.

Upgrade from 3.0/3.1

- ✓ Migrate access control list of user from 3.0/3.1 to 4.0

Access Control Lists

User

- ✓ Maintain user
- ✓ Generate access control list of user
- ✓ Maintain access control list of user
- ✓ Maintain extended access control list of user
- ✓ Assign authorization to RFC user

Systems

- ✓ Maintain access control list for SAP Systems

Communication

Printing using SAPlpd

- ✓ Maintain printer

RFC Remote Function Call

- ✓ Define RFC Destinations
- ✓ Define SNC information of RFC destination

CPIC

- ✓ Define CPIC destination
- ✓ Define SNC information of CPIC destination

External security systems

- ✓ Import user from external security system (planned)
- ✓ Export user for external security system
- ✓ Check canonical SNC names

3.4.1 Upgrade from 3.0/3.1

If you have used SNC to secure SAPgui connections prior to Release 4.0, then you need to:

- **Migrate access control list of user from 3.0/3.1 to 4.0**

  This activity transfers the access control lists for users from the earlier release to Release 4.0 (report RSSNC40A).

3.4.2 Access Control Lists (ACL)

There are two types of access control lists that you need to maintain, a user ACL and a system ACL.

3.4.2.1 User Access Control List

The following activities apply to the user ACL:

- **Maintain user**

  Use this activity to maintain the SNC information for each individual user (transaction SU01, User Maintenance). See *Chapter 3.6: User Maintenance in the SAP System*.

- **Generate access control list of user**

  Use this activity to automatically generate SNC names for users by using a uniform schema that consists of a fixed prefix, the SAP System user ID, and a company-defined suffix. For more information, see the section titled *Use report RSUSR300 to create SNC names* in *Chapter 2.3.2: Naming Conventions.*

- **Maintain access control list of user**

  As an alternative to maintaining the individual users with the transaction SU01, you can use this activity to directly enter users' SNC names in the USRACL table (transaction SM30, view USRACL). See *Chapter 3.6: User Maintenance in the SAP System*.

- **Maintain extended access control list of user**

  Use this activity to assign SNC names to RFC or CPIC users (transaction SM30, view USRACLEXT). See *Chapter 3.6.2: Maintaining SNC Information for Non-Dialog Users.*

- **Assign authorization to RFC user**

  The following authorization objects are especially important when RFC is used between components in SAP Systems:

- S_RFC	Authorization check at RFC access
- S_RFCACL	Authorization check for RFC user

  Use the *Authorization Info System* (transaction SUIM) to make sure that these objects are properly assigned. (Both objects belong to the class *Cross-application Authority Objects*.)

3.4.2.2 System Access Control List

With this activity, you define a system ACL where allow access to SAP Systems according to their SNC names (transaction SNC0 or transaction SM30, view VSNCSYSACL). See *Chapter 4.3.3: RFC: SAP System → SAP System* for details.

3.4.3 Communication

Under *Communication*, we include the Customizing activities for configuring SNC options when using SAPlpd, RFCs, CPICs, and for maintaining information specific to the external security product.

3.4.3.1 Printing using SAPlpd

To assign SNC names to SAPlpd printers, use the activity:

- **Maintain printer**

  See also *Chapter 4.5.2: Printing Using SAPlpd*.

3.4.3.2 RFC Remote Function Call

The following activities apply to using SNC with RFCs:

- **Define RFC Destinations**

  Perform this activity to define RFC destinations (transaction SM59). See *Chapter 4.3: Configuring SNC Options: Using RFC from SAP Systems*.

- **Define SNC information of RFC destination**

  Perform this activity to define the SNC options for RFC destinations (transaction SM30, view RFCDESSECU). See *Chapter 4.3: Configuring SNC Options: Using RFC from SAP Systems*.

3.4.3.3 CPIC

The following activities apply to using SNC with CPICs:

- **Define CPIC Destinations**

  Perform this activity to define CPIC destinations (transaction SM54). For more details, see *Chapter 4.4: Configuring SNC Options: Using CPIC from SAP Systems.*

- **Define SNC information of CPIC destination**

  Perform this activity to define the SNC options for CPIC destinations (transaction SM30, view TXCOMSECU). See *Chapter 4.4: Configuring SNC Options: Using CPIC from SAP Systems.*

3.4.3.4 Maintain the External Security System

The following activities apply to maintaining information that is relevant to the external security system:

- **Import user from external security system (planned)**

  This activity is currently still in development. Once available, you will be able to import user information from the external security product into the SAP System.

- **Export user for external security system**

  Perform this activity to export user information (SNC name) from the SAP System into a file that can be read and used by the external security product's user maintenance (report RSUSR402).

- **Check canonical SNC names**

  This activity runs the report RSSNCCHK, which collects and displays the SNC names that are contained in the various SNC-relevant tables in the SAP System. It performs consistency checks and makes sure that the SNC names exist in canonical form. If names are not represented in canonical form, but can be converted, then it automatically transforms them. Names that cannot be converted are displayed and indicated as such so that you can correct or delete them.

3.5 Transport the Customizing Configuration

For a complete system that consists of several SAP Systems, there are the following possible methods you can use to transport the Customizing configuration:

- Manual entry
- Special functions (for example, transactions, RFC-enabled function modules, Application Link Enabling)
- Compare tables
- Customizing transport
- Copy client

This chapter describes which methods can be used for transporting the SNC configuration information. In the corresponding examples, we describe the system using a delivery system and a target system. The delivery system supplies the Customizing information to the target system. Pay close attention to any notes that are provided.

3.5.1 Upgrade from 3.0/3.1

After upgrading your system from 3.0/3.1, and after you have completed the Customizing activities mentioned in *Chapter 3.4*, the USR15 table is empty. You need to transport this empty table to the target system. To transport the table, you must manually initiate the transport request. The entry in the transport request is as follows:

- Transport objects: `R3TR TABU USR15`
- Key: `<Client>*` or `*`

3.5.2 *Access Control Lists*

3.5.2.1 User Access Control List

- **User**

  To transport user information, use the standard method of copying the client.

- **Access Control of User**

  To transport the table USRACL (Assign SNC names to users), use transaction SM30, view USRACL.

  > Currently, this table is considered application data, and not user information. For each client where you transport user information by means of copying, you must also initiate a transport request for table USRACL.

- **Extended Access Control of User**

  To transport the table USRACLEXT (Assign additional SNC names to users or assign SNC names for RFC users or CPIC users), use transaction SM30, view USRACLEXT.

  > Currently, this table is also considered application data, and not user information. For each client where you transport user information by means of copying, you must also initiate a transport request table USRACLEXT.

- **Authorization for RFC User**

  To transport the user information, use the standard method of copying the client.

3.5.3 *System Access Control List*

To transport the system access control list (table SNCSYSACL - Assign SNC names to systems), use transaction SNC0 or transaction SM30, view VSNCSYSACL, type = E. You do not need to transport internal entries.

> After copying a client, you can delete any superfluous entries in tableSNCSYSACL. Use transaction SM30, view VSNCSYSACL, type = I. Also delete any superfluous external entries (type = E).

3.5.4 Communication

The following sections apply to transporting the various communication settings when using SNC. They include printing using SAPlpd, RFCs and CPICs.

3.5.4.1 Printing using SAPlpd

For information about transporting printer definitions, see the online documentation *BC Printing Guide → Transporting Printers (Device Definitions)* and *Transporting a Device Type* [6].

3.5.4.2 RFC Remote Function Call

You need to manually maintain the RFC destinations in the target system.

3.5.4.3 CPIC

You also need to manually maintain the CPIC destinations in the target system.

3.6 User Maintenance in the SAP System

With SNC, the names of the communication partners as known to the external security product are exchanged in the corresponding SNC layers in the SAP System components. For example, the authentication process for a user logging on to the SAP System over an SNC-protected SAPgui occurs between the SAPgui's SNC layer and the SNC layer on the application server. Because this is a secure authentication procedure, the SAP System can use the SNC name, which is a specialized form of the external user name, to authenticate the user in the SAP System and accept (or deny) the logon request. Therefore, all users, to include both dialog and non-dialog users, need to have identifications in the SAP System that correspond to the user IDs used by the external security product. The next sections explain the user maintenance in the SAP System in more detail.

3.6.1 Maintaining SNC Information for Dialog Users

For each user who logs on to the SAP System using SNC, you must establish a relationship between the SAP System user ID and the external user name (SNC name).

Restrictions

- You can only assign a single SNC name to a user account in the SAP System.

  With this restriction, you can be sure that each user in the SAP System also has a single identity with the external security product. This is necessary for monitoring user actions, for example, for auditing purposes.

- In releases prior to Release 4.5, do not assign the same SNC name to multiple users in a single client in the SAP System. If you do, we cannot guarantee the user will be correctly mapped in the SAP System.

- As of Release 4.5, you can suppress the initial logon screen if the system can map the SNC user name to a single user in the SAP System (provided that the parameter `snc/force_login_screen` = 0). If the SNC name matches several users in the SAP System, then a logon screen appears where the user can select the correct account to use (see *Chapter 3.7: SAP System Logon Screen*).

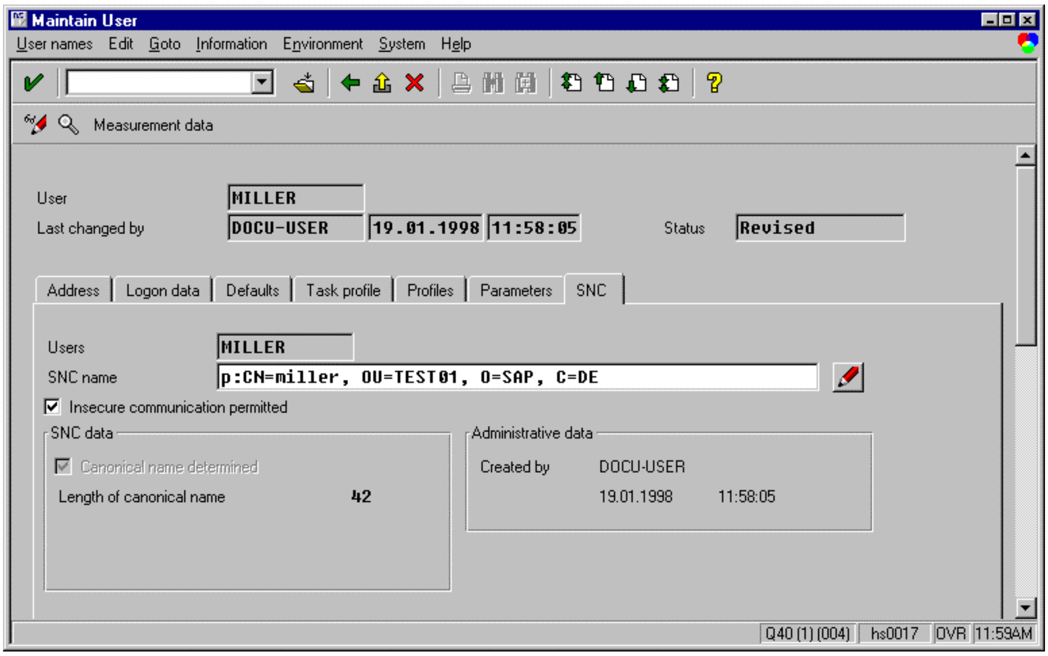
Prerequisites

- SNC needs to be activated in the SAP System (`snc/enable` = 1).

- If you want to allow insecure communications for certain users, then the profile parameter `snc/accept_insecure_gui` must be set to the value "U".

Procedure

To assign the relationship between the user ID in the SAP System and the SNC name, use transaction SU01. See Figure 3-1:



User: MILLER

Last changed by: DOCU-USER 19.01.1998 11:58:05 Status: Revised

Users: MILLER

SNC name: p:CN=miller, OU=TEST01, O=SAP, C=DE

☑ Insecure communication permitted

SNC data

☑ Canonical name determined

Length of canonical name: 42

Administrative data

Created by: DOCU-USER 19.01.1998 11:58:05

Figure 3-1: SNC User Maintenance in the SAP System (Transaction SU01)

1. Enter the SNC name in the *SNC name* field. You can enter a longer name by choosing the icon *Change SNC-Name*.
2. Select *Insecure communication permitted* if you want to allow insecure logons for the user.

   This option is only effective if the profile parameter `snc/accept_insecure_gui` contains the value "U".

3. Save the SNC data.

Result

The SAP System automatically updates the user ACL (table USRACL) and generates the user's SNC name in canonical form. If no errors occurred, then the system activates the *Canonical name determined* indicator and displays the length of the SNC name. An error may occur, for example, if the SNC name contains syntax errors.

As an alternative, you can use transaction SM30, view USRACL, to directly enter the SNC names in the USRACL table.

3.6.2 Maintaining SNC Information for Non-Dialog Users

For communications initiated by external CPIC or RFC programs that are to be protected with SNC, the system also validates the combination of the user ID in the SAP System and the SNC name supplied by the external program.

You can also use transaction SU01 to assign SNC names to RFC or CPIC users. Note, however, with transaction SU01, you can only assign a single SNC name to a user and there may be cases where you want to assign additional SNC names to RFC or CPIC users. For these cases, you can maintain additional SNC names in the extended user ACL (table USRACLEXT).

The extended user ACL is also necessary when protecting WebRFC connections with SNC. In this case, the system uses the AGate's credentials (and the AGate's SNC name) to obtain the information needed to apply SNC protection to the connection. To allow WebRFC users access to the system using the AGate's secure connection, and to enforce their authentication, you need to make a corresponding entry in the USRACLEXT table.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

See the previous section for information on using transaction SU01 to maintain users' SNC information. In this section, we describe how to maintain the SNC information by directly entering the information in table USRACLEXT.

Although it is possible, **we do not recommend entering additional SNC names for dialog users in USRACLEXT**.

Prerequisites

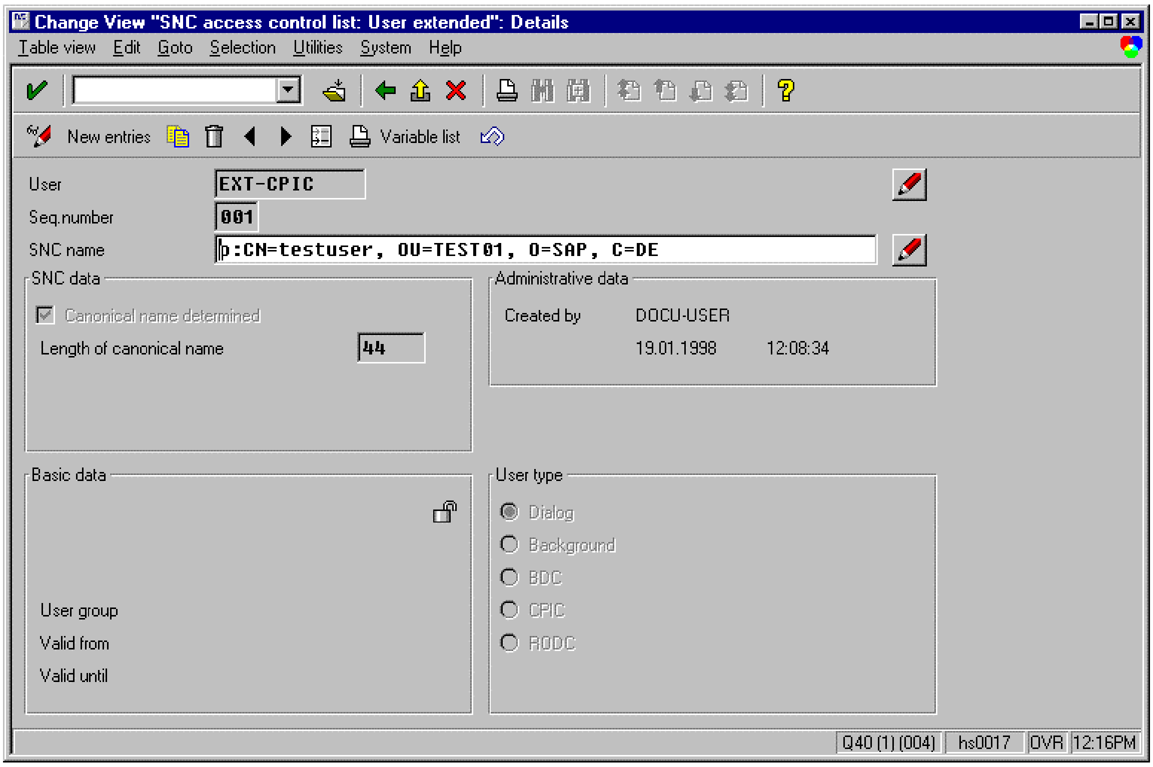
- The user must have a user master record in the SAP System before you can enter the user ID in the table USRACLEXT.
- If you need more than one SNC name for a single user in the SAP System, you must establish a numbering system to distinguish between the different entries.

Procedure

From the table maintenance for table USRACLEXT (for example, use transaction SM30):

1. To change, create or delete entries, choose *Goto* → *Details*, *Edit* → *New Entries*, or *Edit* → *Delete*, respectively.

   When entering changes and creating new entries, the following screen appears:



User EXT-CPIC

Seq.number 001

SNC name p:CN=testuser, OU=TEST01, O=SAP, C=DE

SNC data

☑ Canonical name determined

Length of canonical name 44

Administrative data

Created by DOCU-USER

19.01.1998 12:08:34

Basic data

User group

Valid from

Valid until

User type

● Dialog

○ Background

○ BDC

○ CPIC

○ RODC

Figure 3-2: SNC User Maintenance for Non-Dialog Users (SM30 – USRACLEXT) – Changing or Creating New Entries

2. If you need to create or change the user's master record, choose the *Change User* icon to the right of the *User* field.

3. If the user has more than one SNC name, then enter the appropriate sequence number for the user in the *Seq.number* field (for new entries only).

4. Enter the user's SNC name in the *SNC name* field.

   You can use the asterisk symbol (*) as a wildcard for both the SAP System user name as well as for the SNC name. Note the following:

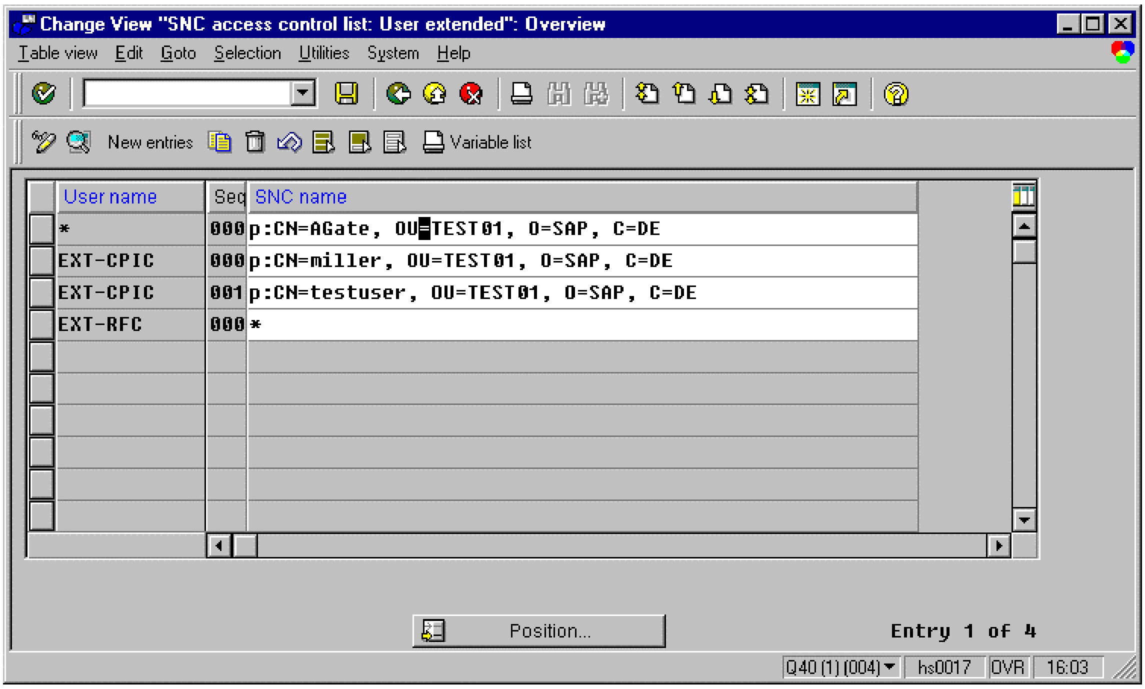
   - If you enter an asterisk for the SAP System user ID, then the system accepts any user in the SAP System that has an SNC name that matches the name entered in the *SNC name* field.
   - If you enter an asterisk for the SNC name, then the system accepts the user with the corresponding SAP System user ID, regardless of his or her SNC name.
   - If you enter an asterisk in both fields, then the system accepts any user with anySNC name.

   If you use the wildcard character in either field, the SAP System performs a password verification at connection time.

   An informational message appears if either of these fields contain the wildcard value.

Examples for Using the Extended User ACL

Figure 3-3 shows the information used in the following examples.



User name	Seq	SNC name
*	000	p:CN=AGate, OU=TEST01, O=SAP, C=DE
EXT-CPIC	000	p:CN=miller, OU=TEST01, O=SAP, C=DE
EXT-CPIC	001	p:CN=testuser, OU=TEST01, O=SAP, C=DE
EXT-RFC	000	*

Figure 3-3: Example Extended User ACL (Transaction SM30 – USRACLEXT)

Example 1: CPIC User

In this example, a CPIC program is used to communicate between two SAP Systems. One possible scenario is to use the initiating SAP System as the SNC communication partner and define an entry for it in the system ACL (table SNCSYSACL). However, an entry in SNCSYSACL establishes complete trust for the system.

Instead of using SNCSYSACL, you can use the USRACLEXT table to allow the communication to run under specific accounts only. In Figure 3-3, the CPIC user EXT-CPIC is used for communicating between the two SAP Systems; however, only the users with the corresponding SNC names for `miller` and `testuser` are allowed to connect as EXT-CPIC.

Example 2: WebRFC User

To use SNC to protect the communication path between the ITS AGate and the SAP System application server, you need to create an entry for the AGate in the SNC system ACL (table SNCSYSACL). The system then allows the AGate to establish an SNC-prtoected connection to the SAP System application server. It uses the AGate's credentials to authenticate the AGate and to set up the SNC-protected connection.

WebRFC users then need access to the SAP System using the AGate's SNC-protected connection. The first USRACLEXT entry shown in Figure 3-3 allows users (that is, the WebRFC users) to connect to the SAP System using the AGate's connection. The users themselves are explicitly authenticated at connection time.

3.7 SAP System Logon Screen

As of Release 4.5, you have the option of suppressing the normal logon screen for anSNC-protected logon request – if possible. The logon screen is suppressed if the following criteria are met:

- The profile parameter `snc/force_login_screen` is set to the value "0".
- The system can uniquely determine the user ID and client in the SAP System.

  This is only possible if only one user ID exists in the SAP System with the correspondingSNC name, and this user exists in only one SAP System client. In this case, the SAP System can uniquely determine the user and the SAP System client and can log the user on without requiring any additional information.

  If the SAP System cannot uniquely determine the user and client in the SAP System, then it produces the logon screen and requests the information needed to complete the logon.

If the profile parameter is set to the value "1", then the SAP System automatically displays the logon screen at every logon attempt.

4 Configuring the Communication Partners for Use with SNC

In this chapter, we describe how to configure SNC for the SAP System components involved in the various communications. For most of the communication paths, we define one of the partners as the initiator of the communication and the partner as the acceptor. In certain cases, such as the communication between two SAProuters, the components can act as both the initiator as well as the acceptor.

4.1 Configuring SNC Options: SAPgui → SAP System

For the communication between the SAPgui and the SAP System, the SAPgui is the initiator of the communication and the SAP System is the acceptor.

Initiator (SAPgui)

There are several ways to start SAPgui. They are:

- Direct start (execute `sapgui.exe` from a command prompt or over a shortcut)
- SAP Logon
- SAP Shortcuts
- SAP Session Manager

You can use SNC between the SAPgui and the SAP System if you start SAPgui directly, use SAP Logon, or SAP Shortcuts; however, the SAP Session Manager does not support SNC at this time. We describe the SNC configuration for each of the supported start methods below.

Direct Start

In all of the supported operating system environments, you can establish a SAPgui connection by executing `sapgui.exe` from the command prompt. Under Windows, it is customary to set up a shortcut on the desktop.

To be able to establish an SNC-protected connection between SAPgui and the SAP System, you need to set the SNC parameters either in environment variables or in the command line. Table 4-1 shows these parameters and where you can set each of them.

Table 4-1: SNC Command Line Parameters for SAPgui → SAP System

Parameter	Short Description	Required or optional	Permitted Values	Default	Where to set
Release 3.1 frontend software					
`SNC_LIB`	Path and file name of the gssapi library	Required	String value (no quotation marks)	None	Environment variable
`SNC_QOP`	Quality of protection (protection level)	Optional	1,2,3 (all Releases) 8,9 (Release 3.1I)	3	Environment variable
`/snc`	SNC name of the application server	Required	String value (no quotation marks)	None	Command line
as of Release 4.0 frontend software					
`SNC_PARTNERNAME`	SNC name of the application server	Required	String value in quotation marks	None	Command line
`SNC_LIB`	Path and file name of the gssapi library	Required	String value in quotation marks	None	Command line or Environment variable
`SNC_MODE`	SNC activation indicator	Optional	1, 0	1, if `SNC_PARTNERNAME` is set	Command line
`SNC_QOP`	Quality of protection (protection level)	Optional	1,2,3,8,9	3	Command line or Environment variable

Note the following:

- In Release 3.1, you can define the `SNC_LIB` and `SNC_QOP` parameters in environment variables only. As of Release 4.0, you can either define them in environment variables or include them in the command line. Values from the command line override values in environment variables.
- In Releases 3.1G/H, the quality of protection (`SNC_QOP`) values 8 (use default) and 9 (use max. available) are not supported for the SAPgui ←→ SAP System connection.
- As of Release 4.0, you need to place the parameter values for `SNC_PARTNERNAME` and `SNC_LIB` in quotation marks ("). In Release 3.1, you only need to include the quotation marks if the parameter values contain spaces.
- In Release 4.0, the parameter `/snc` has been replaced by `SNC_PARTNERNAME`.

The following are examples of the command line entry to start SAPgui:

Release 3.1 frontend software: (Windows 9x or Windows NT)

In this example, we define the location of the shared library in the environment variable `SNC_LIB` and the level of protection in the environment variable `SNC_QOP`. We then establish a connection to the application server `hs0017` using the command line entry `sapgui.exe`.

Setting environment variables:

```
set SNC_LIB=C:\SECUDE\LIB\SECUDE.DLL
set SNC_QOP=3
```

Starting SAPgui:

```
sapgui.exe hs0017 01 /snc="p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE"
```

The application server's SNC name is: `p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE`. The level of protection is 3, indicating that authentication, integrity, and privacy protection should be applied to the connection.

As of Release 4.0 frontend software: (Windows 9x or Windows NT)

In this example, we set all of the parameters in the command line:

```
sapgui.exe hs0017 01 SNC_PARTNERNAME="p:CN=sap01.hs0017, OU=TEST01,
O=SAP, C=DE" SNC_QOP=9 SNC_LIB="C:\SECUDE\LIB\SECUDE.DLL"
```

The connection is established to the application server `hs0017`. The application server's SNC name is: `p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE`. The level of protection is 9, indicating that the maximum level of protection should be applied to the connection, and the shared library is located at: `C:\SECUDE\LIB\SECUDE.DLL`.

SAP Logon

If you use SAP Logon to start SAPgui, then you do not have to set up the command line yourself.

To use SAP Logon to start SAPgui with SNC protection, you need to use a SAP System kernel Release 3.1I (patch level 102) or higher.

Prerequisites

The environment variable `SNC_LIB` on the front end needs to contain the path and file name of the external library.

Procedure

You need to set the SNC options (SNC name, quality of protection, SNC activation) for the application server with which you want to communicate. Make these settings in the SAP Logon *Advanced Options*.

There are slight differences when defining the SNC options depending on the method used to select the application server. The standard server selection methods are:

A. Manual Entry (or edit an existing entry)

B. Entry Using Server Selection

C. Entry Using Group Selection

We describe the details for defining the SNC options for each method below:

SNC-enabled logon destinations are indicated in the SAP Logon destination list using a special icon.

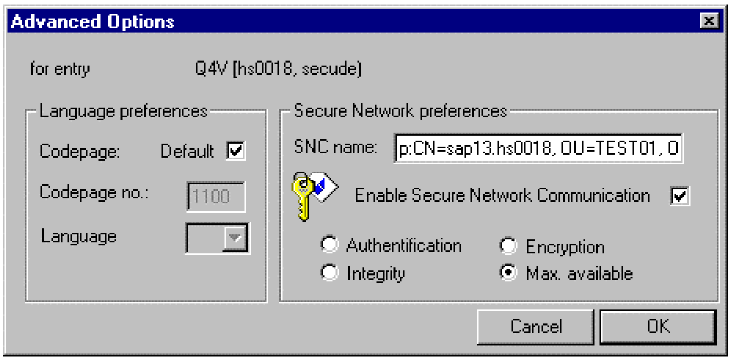
A. Manual Entry (or edit an existing entry)

From the SAP Logon dialog:

1. Choose *New* or *Edit* (or *Properties*, depending on release).
2. Choose *Advanced Options*.

   The *Advanced Options* dialog appears (see Figure 4-1).
3. Enter the SNC options:
   a) Enter (or edit) the *SNC name*.
   b) Enable SNC by activating the *Enable Secure Network Communication* indicator.
   c) Choose the Quality of Protection level that you desire (*Authentication*, *Integrity*, *Encryption*, *Max. available*).

   We recommend you use the default level (*Max. available*).
3. Choose *OK*.



for entry Q4V [hs0018, secude]

Codepage: Default ☑

Codepage no.: 1100

Language

SNC name: p:CN=sap13.hs0018, OU=TEST01, O

Enable Secure Network Communication ☑

○ Authentification ○ Encryption
○ Integrity ● Max. available

Figure 4-1: SAP Logon SNC Options (4.0B Front End)

B. Entry Using Server Selection

After adding the server using *ServersSel.*, configure and activate SNC in the *Advanced Options* dialog box in the same way as with a manual entry (see the previous section). If the server is SNC-enabled at the time of selection, then the application server's SNC name is automatically retrieved by the message server and displayed in the *SNC name* field.

C. Entry Using Group Selection

After adding the server using *Groupsel.*, configure and activate SNC in the *Advanced Options* dialog box in the same way as with a manual entry. Note however, you can only enter the SNC options if SNC has already been activated for the group. In addition, although the *SNC name* field shows the SNC name of a server, this name is not actually used and you cannot edit it. With group logons, the application server's SNC name is dynamically requested by the message server each time a SAPgui is started.

SAP Shortcuts

SAP Shortcuts are available as of Release 4.5. They establish a quick and easy connection to the SAP System for specific transactions. The SAP Shortcut establishes the connection to the corresponding SAP System using information from SAP Logon. Therefore, if you have SNC activated in SAP Logon for the corresponding SAP System, then the connection established by the SAP Shortcut will also use SNC protection.

The SAP Shortcut requests a password, which you can either save in the SAP Shortcut or enter at connection time. Normally, we do not recommend saving passwords in SAP Shortcuts because the logon information is saved locally on the front end and easily accessible. However, to use SNC with a SAP Shortcut, you **have** to save a password in the logon information.

> This password is only necessary to make SAP Shortcuts work for SNC-enabled systems and is not actually used for authentication purposes. The system uses the SNC authentication mechanisms instead. Therefore, to make SAP Shortcuts work for SNC-enabled systems without weakening security, we recommend you save a **single letter password** in the SAP Shortcut. A single letter suffices to use SNC with the SAP Shortcut and it can never be used as a valid password in SAP Systems.

SAP Session Manager

SNC is currently not supported by the SAP Session Manager.

Acceptor (SAP System)

To configure the acceptor (the SAP System) for using SNC, set the profile parameter settings on the application server and define the entries in user maintenance as described in *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server* and *Chapter 3.6: User Maintenance in the SAP System.*

Processing the Logon

When a user logs on to the SAP System when using SNC protection, the logon process continues as follows:

1. The system displays an initial SAPgui screen where the user only has to enter the desired SAP System client and language.

   As of Release 4.5, the logon screen is suppressed if the profile parameter `snc/force_login_screen` = 0 and the system can map the logon to a single user ID in a single client in the SAP System.
2. The SAP System verifies that the user has a user ID in the client requested, and that this user ID possesses the SNC name that corresponds to the external name provided by the security product.
3. If an SNC name is found that corresponds to the external name, the logon proceeds successfully; if not, the user receives an error message.

The system does not accept any logon attempts that are not protected with SNC unless:

- Unprotected logon attempts are generally allowed (`snc/accept_insecure_gui` = 1), or
- Unprotected logon attempts are allowed for specific users (`snc/accept_insecure_gui` = U) and the user logging on has the appropriate permission set in his or her user master record.

4.2 Configuring SNC Options: External Programs → SAP Systems

In this section, we describe the SNC configuration for the communication from external programs to SAP Systems using either RFC or CPIC.

4.2.1 External Programs → SAP Systems Using RFC

For the communication path from an external program to a SAP System when using RFC, the external program is the initiator of the communication and the SAP System is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (external Program)

To apply SNC protection to external programs that communicate with SAP Systems using RFC, you need to specify the SNC options in either the `saprfc.ini` file or over the program interface in `rfclib`. This section describes how to specify the information in `saprfc.ini`. For information on using `rfclib`, see *Chapter 4.9: C Program Interfaces*.

Prerequisites

- You want to apply SNC protection to the communications between the RFC external program and the SAP System.
- The external program uses the `saprfc.ini` file.

Procedure

Set the SNC parameters shown in Table 4-2 in `saprfc.ini`:

Table 4-2: SNC Parameters for RFC External Programs → SAP Systems

Parameter	Description	Required or optional	Permitted Values	Default
SNC_PARTNERNAME	SNC name of the communication partner (application server)	Required	String value	None
SNC_LIB	Path and file name of the gssapi library	Required	String value	None
SNC_MODE	SNC activation indicator	Required	0, 1 0=SNC disabled 1=SNC activated	None
SNC_QOP	Quality of protection (protection level)	Optional	1,2,3,8,9	3
SNC_MYNAME	SNC name of the user sending the RFC	Optional	String value	The name provided by the security product reflecting the logged-on user.

Example destination in the `saprfc.ini` file:

```
DEST=Q40_S
TYPE=A
ASHOST=hs0017
SYSNR=01
SNC_MODE=1
SNC_PARTNERNAME=p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE
SNC_LIB=I:\SECUDE\LIB\secude.dll
```

This example sets up the application server `hs0017` as the RFC destination. The server's SNC name is `p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE` and the SNC library is located at `I:\SECUDE\LIB\secude.dll`.

Acceptor (SAP System)

To configure the acceptor (the SAP System) for using SNC, set the profile parameters on the application server as described in *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*.

The value contained in the parameter `snc/accept_insecure_rfc` determines whether or not to accept unprotected RFC connections. You can define this parameter to deny all insecure RFCs, accept all insecure RFCs, or accept insecure RFCs for specific users only (based on the *Insecure communications permitted* indicator in the table USRACL).

User Authentication in the SAP System

As with RFC calls without SNC protection, you need to specify a user and client in the RFC program when connecting to the SAP System. The following additional steps apply to the authentication procedure when using SNC:

1. If the SNC name from the RFC program corresponds to the SNC name in the specified user's master record in the designated client, then the SAP System accepts the RFC logon request (without performing additional authentication).
2. Otherwise, the SAP System searches the USRACLEXT table for an entry corresponding to the client, user, and SNC name combination. If a matching entry is found, then the SAP System accepts the logon request (without performing additional authentication).
3. Otherwise, the SAP System searches the USRACLEXT table for an entry corresponding to the client, user, and an asterisk (*) as the SNC name. If a matching entry is found, then the system verifies the user's password. If the password is valid, then the SAP System accepts the logon as a secure logon.
4. Otherwise, the SAP System searches the USRACLEXT table for an entry corresponding to the client, an asterisk as the user ID, and the RFC program's SNC name. If a matching entry is found, then the system verifies the user's password. If the password is valid, then the SAP System accepts the logon as a secure logon.
5. Otherwise, the SAP System searches the USRACLEXT table for an entry corresponding to the client, an asterisk as the user ID, and an asterisk as the SNC name. If a matching entry is found, then the system verifies the user's password. If the password is valid, then the SAP System accepts the logon as a secure logon.
6. Otherwise, the SAP System denies the logon request.

When establishing the RFC connection:

The RFC connection is established over a gateway port. For SNC-protected connection requests, the RFC library normally uses the "secure" gateway port, which accepts only SNC-protected connections. However, in Releases 4.0 and 4.5, if both SNC and load-balancing are used, the RFC libraries also use the conventional gateway port for SNC-protected connections.

4.2.2 External Programs → SAP Systems Using CPIC

For the communication path from an external program to a SAP System when using CPIC, the external program is the initiator of the communication and the SAP System is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (external Program)

To apply SNC protection to external programs that communicate with SAP Systems using CPIC, you need to specify the SNC options in either the `sideinfo` file or over the program interface in `cpictlib`. This section describes how to specify the information in the `sideinfo` file. For information on using `cpictlib`, see *Chapter 4.9: C Program Interfaces.*

Prerequisites

You want to apply SNC protection to the communications between the CPIC external program and the SAP System.

Procedure

Set the SNC parameters shown in Table 4-3 in the `sideinfo` file:

Table 4-3: SNC Parameters for CPIC External Programs → SAP Systems

Parameter	Description	Required or optional	Permitted Values	Default
`SNC_PARTNERNAME`	SNC name of the application server	Required	String value in quotation marks	None
`SNC_LIB`	Path and file name of the gssapi library	Required	String value	None
`SNC_MODE`	SNC activation indicator	Required	0, 1 0=SNC disabled 1=SNC activated	None
`SNC_QOP`	Quality of protection (protection level)	Optional	1,2,3,8,9	3
`SNC_MYNAME`	SNC name of the user sending the CPIC	Optional	String value	The name provided by the security product reflecting the logged-on user.

Example destination in the `sideinfo` file:

```
DEST=Q40_S
PROTOCOL=I
LU=hs0017
TP=sapdp01
GWHOST=hs0017
GWSERV=sapgw01s
CPIC_TRACE=1
SNC_PARTNERNAME="p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE"
SNC_MODE=1
SNC_LIB=/usr/local/secude/lib/libsecude.sl
```

This example sets up the application server `hs0017` as the CPIC destination. The server's SNC name is `p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE` and the SNC library is located at: `/usr/local/secude/lib/libsecude.sl`.

Acceptor (SAP System)

Set the profile parameters on the application server as described in *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*.

The value contained in the parameter `snc/accept_insecure_cpic` determines whether or not to accept unprotected CPIC connections. You can define this parameter to deny all insecure CPICs, accept all insecure CPICs, or accept insecure CPICs for specific users only (based on the *Insecure communications permitted* indicator in the table USRACL).

User Authentication in the SAP System

As in CPIC calls without SNC protection, you need to specify a user and client in the CPIC program when connecting to the SAP System. The authentication procedure is identical to that for RFCs (see *Chapter 4.2.1: External Programs → SAP Systems Using RFC*).

CPIC calls can only be performed with user accounts in the SAP System of type CPIC.

When establishing the CPIC connection:

The CPIC connection is established over a gateway port. For SNC-protected connections, you should use the "secure" gateway port. Specify the secure port in the parameter `GWSERV` in the `sideinfo` file. The "secure" port has the character **s** included in the name (see below):

normal port: `GWSERV=sapgw01`

secure port: `GWSERV=sapgw01s`

4.3 Configuring SNC Options: Using RFC from SAP Systems

To use SNC with RFC calls from SAP Systems, you must configure the SNC options for each RFC destination individually. You can either use transaction SM59 or SM30 (table RFCDESSECU). In this chapter, we describe the procedures using transaction SM59.

Transaction SM59 distinguishes the following types of RFC destinations:

- R/2 connections
- R/3 connections
- Internal connections (created automatically and cannot be maintained)
- Logical destinations
- Connections to external programs (TCP/IP connections)

The maintenance of the SNC options for the initiating side of the communication (SAP System) is similar for all of these categories and is described in the following section, *4.3.1: Maintaining RFC Destinations and their SNC Options Using Transaction SM59.* The specifics, along with the options to set for the accepting side, are described in the further sections, *4.3.2 - 4.3.15*.

4.3.1 Maintaining RFC Destinations and their SNC Options Using Transaction SM59

Use transaction SM59 to maintain RFC destinations and their SNC options.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

When maintaining the SNC options for RFC destinations using transaction SM59, you specify the following SNC information:

- SNC mode for the connection (active or inactive)
- Quality of protection (QoP)
- SNC partner name

The other SNC-relevant settings (the application server's SNC name, the location of the external library, the maximum quality of protection, and the default quality of protection) are applied as defined in the application server's instance profile (see *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*).

If the RFC destination is an external RFC server program (*Activation type = Start*), then note the following:

- If you specify the external server program to start on an explicit host, then you need to specify the SNC name of the partner host in the SNC options to use SNC for the connection.
- If you specify the external server program to start on the application server or on the frontend workstation, then the SNC name of the partner is automatically derived from an existing secure path and you do not need to specify the SNC name of the partner in the SNC options. (In this case, the field for the SNC name is not activated.)

Prerequisites

Before you can maintain the SNC information, the RFC destination must be defined and SNC activated on the application server.

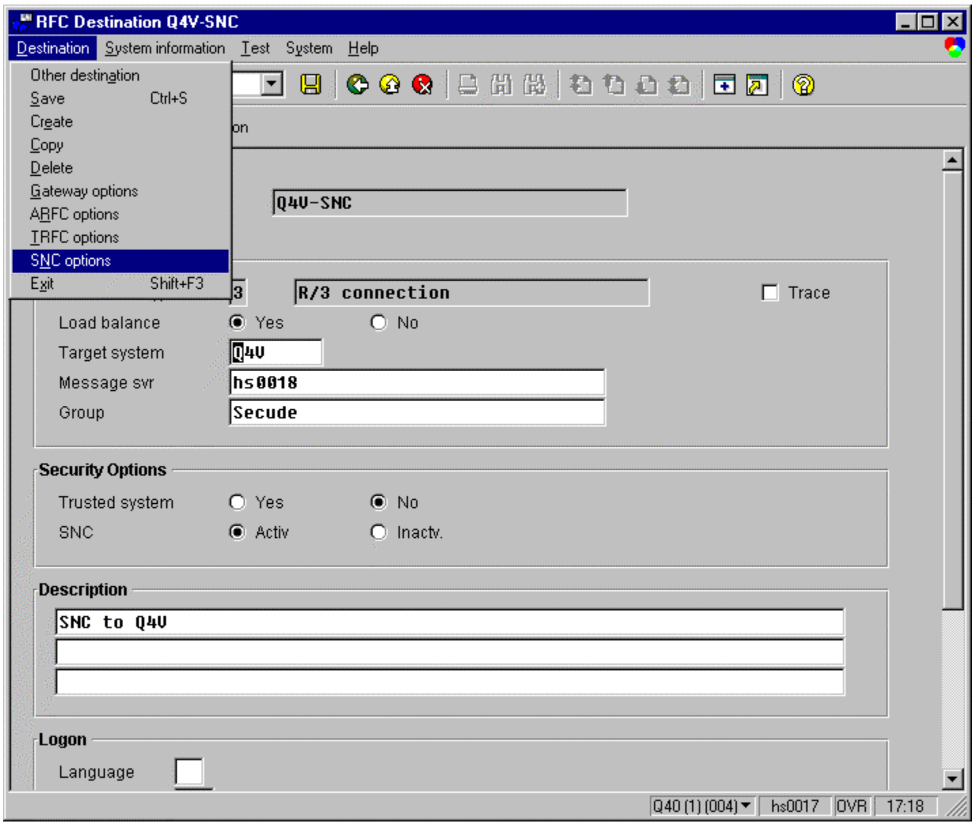
Procedure

From the *Display and maintain RFC destinations screen* (transaction SM59):

1. Place the cursor on the destination application server and choose *Change*.
2. To enable SNC, select the *SNC Activ* indicator.
3. Choose *Destination* → *SNC Options* (see Figure 4-2).

   The *Change View "SNC extension: Details"* screen appears (see Figure 4-3).

   Enter the quality of protection in the *QOP* field.
4. Unless the destination is an external program that starts on the frontend workstation (see the note above), enter the SNC name of the communication partner in the *SNC names* group.
5. Save the data.



Q4V-SNC

3 R/3 connection ☐ Trace

Load balance ● Yes ○ No

Target system Q4V

Message svr hs0018

Group Secude

Security Options

Trusted system ○ Yes ● No

SNC ● Activ ○ Inactv.

Description

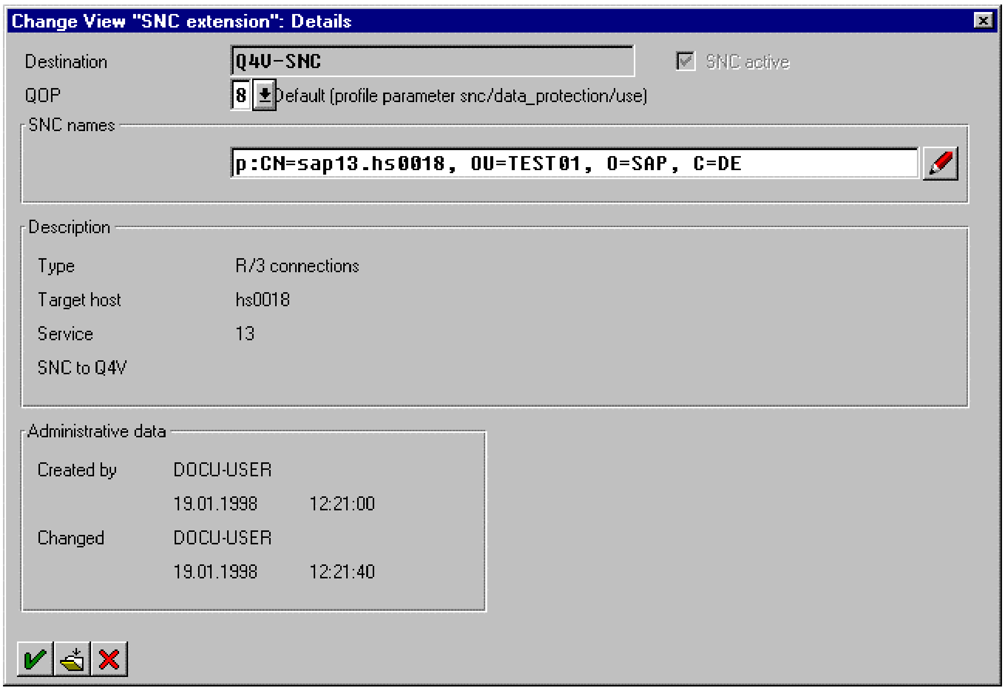
SNC to Q4V

Logon

Language

Q40 (1) (004) hs0017 OVR 17:18

Figure 4-2: Activating SNC for RFC Destinations



Change View "SNC extension": Details

Destination Q4V-SNC ☑ SNC active

QOP 8 Default (profile parameter snc/data_protection/use)

SNC names

p:CN=sap13.hs0018, OU=TEST01, O=SAP, C=DE

Description

Type	R/3 connections
Target host	hs0018
Service	13
SNC to Q4V	

Administrative data

Created by	DOCU-USER	
	19.01.1998	12:21:00
Changed	DOCU-USER	
	19.01.1998	12:21:40

Figure 4-3: SNC Options for RFC Destinations

Quality of Protection (QoP)

The following rules apply to the relationship between the QoP entered in the above screen and the QoP configured in the application server's profile parameter:

- The RFC destination's QoP can be smaller than the application server's `snc/data_protection/min` or larger than the application server's `snc/data_protection/max`.
- If the RFC destination's QoP is larger than the level provided by the external security product, then the largest possible QoP is used.
- If the RFC destination's QoP = 8 (default), then the QoP value from the application server's `snc/data_protection/use` is used.
- If the RFC destination's QoP = 9 (maximum), then the QoP value from the application server's `snc/data_protection/max` is used.

There are a few differences to these rules in Release 4.0A. They are described in *Appendix D: Special Cases Relevant to Releases 3.1G/H and 4.0A*.

Set the QoP to either 8 (default) or 9 (maximum value).

4.3.2 RFC: SAP System → R/2

SNC protection for connections to R/2 is **not** supported.

4.3.3 RFC: SAP System → SAP System

For the communication path between two SAP Systems when using RFC, the calling SAP System is the initiator of the communication and the SAP System defined as the RFC destination system is the acceptor. Settings that are relevant for load balancing are made in the initiating SAP System.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiating SAP System, use transaction SM59. See*Chapter 4.3.1: Maintaining RFC Destinations and their SNC Options Using Transaction SM59*. Depending on whether or not you use load balancing, note the following:

- **Without load balancing**

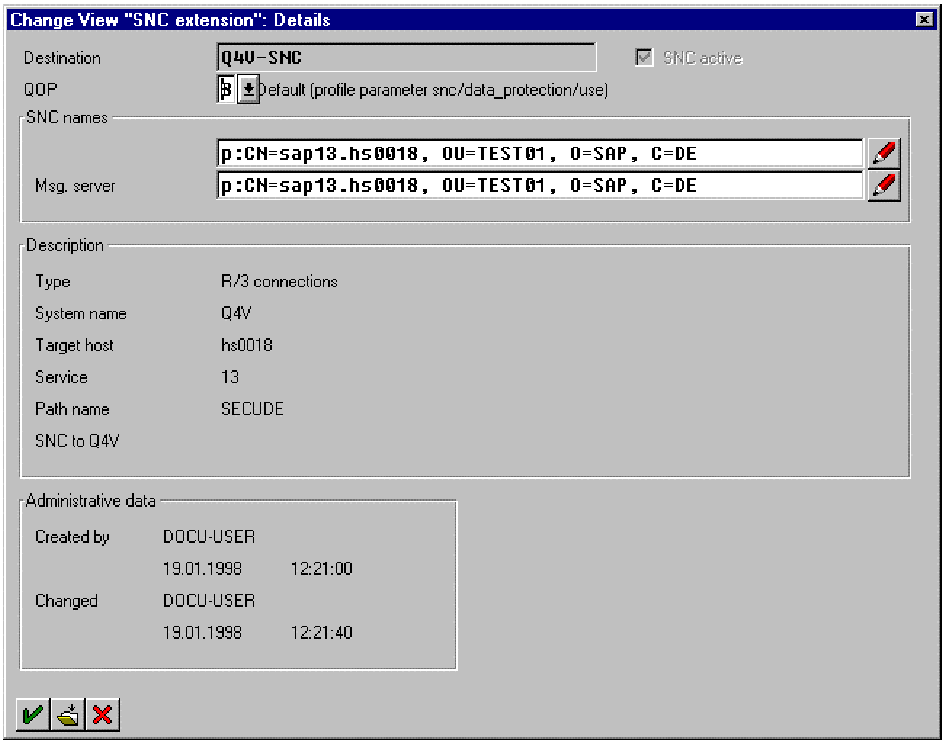
  If you do not use load balancing, then specify the SNC name of the destination application server in the *SNC names* group (see Figure 4-3).

- **With load balancing**

  If you use load balancing, the system (re-)determines the destination application server at the time of the RFC call. After determining the application server, the system retrieves the corresponding application server's SNC name from the message server and uses it to establish the SNC-protected communication.

  In this case, enter the SNC name of the main instance in the *Msg.-Server* field (see Figure 4-4). In the current implementation, the SNC name is parsed as a name, but is not used.

  To configure the system to use the SNC name of a specific application server in case you disable load balancing, enter the desired application server's SNC name in the unlabeled field. As long as you use load balancing, the system ignores the contents of this field.



Change View "SNC extension": Details

Destination: Q4V-SNC

☑ SNC active

QOP: 8 Default (profile parameter snc/data_protection/use)

SNC names

p:CN=sap13.hs0018, OU=TEST01, O=SAP, C=DE

Msg. server: p:CN=sap13.hs0018, OU=TEST01, O=SAP, C=DE

Description

Type	R/3 connections
System name	Q4V
Target host	hs0018
Service	13
Path name	SECUDE
SNC to Q4V	

Administrative data

Created by	DOCU-USER	
	19.01.1998	12:21:00
Changed	DOCU-USER	
	19.01.1998	12:21:40

Figure 4-4: SNC Options for RFC Destinations: SAP System Connection with Load Balancing

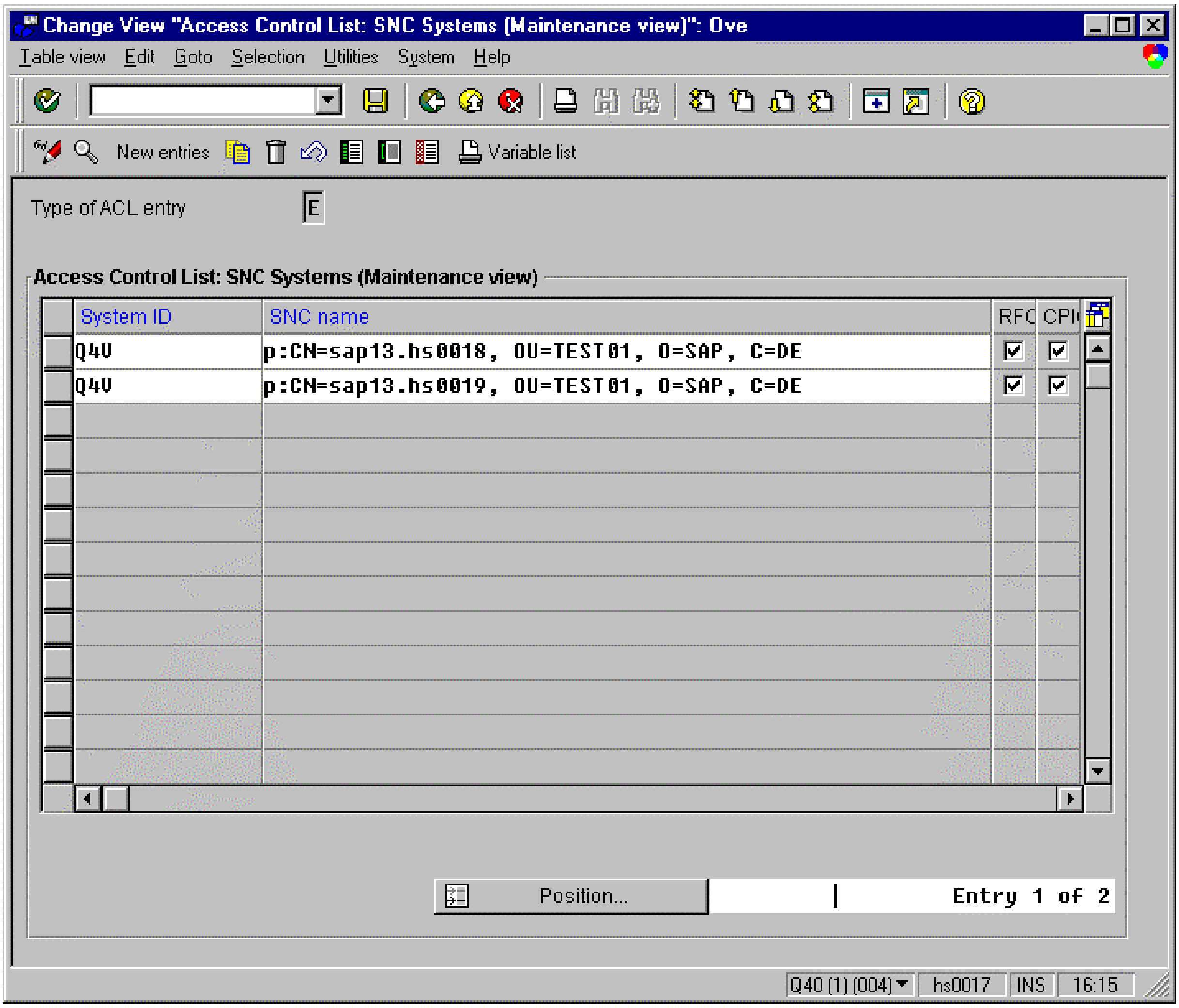
Acceptor (SAP System)

To be able to receive SNC-protected RFCs from other SAP Systems, you need to specify the corresponding systems in the SNC system ACL. In the accepting SAP System:

1. Call transaction SNC0 to maintain entries in the SNC system ACL (table SNCSYSACL; see Figure 4-5).
2. Create an entry **for each application server** from other SAP Systems that needs RFC access to this SAP System. To create an entry, choose *Edit* → *New entries*; to modify an existing one, choose *Goto* → *Details*.

   If you have multiple application servers in a remote SAP System that use different credentials (different SNC names), you need to make an entry for **each** application server in the table SNCSYSACL.

   The table maintenance screen appears.
3. Enter the *System ID* and *SNC name* of the initiating SAP System in the corresponding fields.
4. Activate the *Entry for RFC activated* indicator.
5. If CPIC connections are also to be accepted for this connection, then also activate the *Entry for CPIC activated* indicator.
6. Save the data.



Change View "Access Control List: SNC Systems (Maintenance view)": Ove
Table view Edit Goto Selection Utilities System Help
New entries
Variable list
Position...

Type of ACL entry E

Access Control List: SNC Systems (Maintenance view)

System ID	SNC name	RFC	CPI
Q4V	p:CN=sap13.hs0018, OU=TEST01, O=SAP, C=DE	☑	☑
Q4V	p:CN=sap13.hs0019, OU=TEST01, O=SAP, C=DE	☑	☑

Entry 1 of 2

Q40 (1) (004) hs0017 INS 16:15

Figure 4-5: Access Control List for SNC-protected RFCs from other SAP Systems

Note the following:

- The SNCSYSACL entries that you make using transaction SNC0 are saved as external RFC destinations (type = E). Internal destinations (type = I) are automatically generated and not shown in transaction SNC0.
- If RFCs are to occur within a single SAP System as "external RFCs" to itself (meaning that you defined the RFC destination with the type *R/3 connections* in transaction SM59), then you need to create an external destination entry (type = E) in addition to the automatically generated internal entry (type = I).
- In addition, you need to specify whether the accepting SAP System should accept RFCs that do not use SNC protection. To allow insecure RFC connections, set the profile parameter `snc/accept_insecure_rfc` to the value "1" (see *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*).

System and User Authentication

When using SNC-protected RFCs between two SAP Systems, the application server from one system uses SNC to authenticate the application server of the other system. Based on the entries in SNCSYSACL (SNC name of the application server making the call), the accepting application server recognizes that the RFC call was initiated by another SAP System. The accepting SAP System then uses the standard RFC password or token-based authentication to apply the correct user account and authorizations to the RFC call.

User A in System Q4V (application server `hs0018`) performs an RFC call to System Q40 (application server `hs0017`). Based on the information in the SNCSYSACL table (see Figure 4-5), the system Q40 uses SNC to authenticate the system Q4V. The system Q40 then authenticates User A using the standard authentication mechanism (password or token) that was provided with the RFC request.

4.3.4 RFC: Internal Destinations

At start-up, the SAP System automatically generates the RFC internal destinations to application servers within the system (type = I). The system also automatically makes their respective entries in the table SNCSYSACL. You cannot manually maintain these entries.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

For performance reasons, we do not recommend using SNC for internal destinations! (See *Chapter 2.6: Recommendations.)*

If you do want to secure RFCs to internal destinations with SNC, then set the parameters `snc/r3int_rfc_secure` and `snc/r3int_rfc_qop` in the initiating SAP System application server's profile (see *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*). Make sure that these parameters are identically set for the various application servers that are to use RFCs to internal destinations.

If internal RFCs are not to be protected with SNC (`snc/r3int_rfc_secure = 0`), then leave the profile parameter `snc/accept_insecure_r3int_rfc` to its default value "1". Otherwise, you cannot use internal RFCs and your system will not function correctly.

For incoming RFCs to internal destinations, the system does verify the entry in the SNCSYSACL table. This entry is automatically created as an internal destination (type = I) at start-up, based on the information located in the above mentioned profile parameters.

4.3.5 RFC: Logical Destinations

All logical destinations refer to an actual physical destination. The SNC protection for RFCs to logical destinations is therefore applied according to the SNC options assigned to the corresponding physical destination.

4.3.6 RFC: TCP/IP Connection - Start an External Program on an Application Server

For an RFC destination of type *TCP/IP connection* that is configured to start an RFC server program on an application server, the work process that calls the RFC server program starts the program directly. Once the RFC server program is running, it establishes a TCP communication channel back to the application server's gateway. To establish this channel, the program uses the parameter values that it received over the command line upon process creation.

When SNC is active, the work process that starts the program sends the SNC information to the RFC server program in additional parameters. Therefore, the external server program can use the application server's SNC configuration and credentials to protect the TCP-based communication channel with SNC.

In this scenario, the SAP System is the initiator of the communication and the external program is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM59. See *Chapter 4.3.1: Maintaining RFC Destinations and their SNC Options Using Transaction SM59*.

Acceptor (external program)

You do not need to specify any additional SNC options for external programs that start on an application server. The programs retrieve the SNC information that they need as follows:

- SNC mode and QoP

  The SNC mode (active or inactive) for the connection and the quality of protection are defined in transaction SM59 for the initiator and automatically sent to the program to be started.

- Name and location of the external library

  The external program finds the name and location of the external library (`SNC_LIB`) in the application server's profile parameter `snc/gssapi_lib`.

- SNC name for the external program

  The SAP System uses the SNC name of the application server where the program is started as the SNC name for the external program. The external program is a child process of a work process on the application server and therefore has the identical security environment as the parent work process. This is the only way the SAP System make sure that a valid SNC name is provided for an external program that may run on several different application servers.

4.3.7 RFC: TCP/IP Connection - Start an External Program on an Explicit Host

An external RFC server program started on an explicit host is started directly by a gateway and therefore has access to the same environment as the gateway.

For an RFC call that uses a TCP/IP connection to start an external program on an explicit host, the SAP System is the initiator of the communication and the external program is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM59. See *Chapter 4.3.1: Maintaining RFC Destinations and their SNC Options Using Transaction SM59*.

If you do not specify a gateway in the RFC destination maintenance, then the external RFC server program is started by the application server's standard gateway. This constellation is very similar to that described in *Chapter 4.3.6: RFC: TCP/IP Connection - Start an External Program on an Application Server*. However, in this case, the system ignores the SNC partner name as defined in the RFC destination's SNC options and uses the application server's SNC name as the SNC name for the external RFC server program instead.

Acceptor (external program)

You do not need to specify any additional SNC options for external programs that start on an explicit host. The programs retrieve the SNC information that they need as follows:

- SNC mode and quality of protection

  The SNC mode (active or inactive) for the connection and the quality of protection are defined in transaction SM59 for the initiator and are automatically sent to the program to be started.

- Name and location of the external library

  To specify the path and file name of the external library, the gateway that starts the external RFC server program sends the value of its own profile parameter `snc/gssapi_lib` to the external program as a command line parameter. (This command line parameter value overrides the `SNC_LIB` environment variable value.)

- SNC name for the external program

  The RFC server program's SNC name is the name defined as the SNC partner name in the RFC destination (using transaction SM59). It is sent to the external RFC server program in the RFC request. The external RFC server program extracts this name from the SNC protocol that frames the RFC request and uses it to acquire its accepting credentials.

Gateway Operations

See *Chapter 3.3: Profile Parameter Settings on the Gateway* for information pertaining to SNC with gateway operations.

In addition, note the following:

- Make sure that SNC is activated for the gateway (`snc/enable` = 1) and that the path and file name of the external library are contained in the profile parameter `snc/gssapi_lib`.
- As default, external programs without SNC protection will not be started by the gateway. To enable the starting of external programs without using SNC protection, set the gateway's profile parameter `snc/permit_insecure_start` to the value "1".
- When using SNC, we recommend having the gateway start external RFC server programs locally and **not** on remote hosts. Disable the starting of programs on remote hosts as described in *Chapter 3.3: Profile Parameter Settings on the Gateway*.

  The gateway uses the common Berkeley remote shell (`rsh` or `remsh`) to start programs on remote hosts. The Berkeley remote shell performs only a simple authentication based on the IP address and cannot protect the TCP datastream that it uses. Therefore, we recommend that you do not use the starting of programs on remote hosts when using SNC.
- However, if the RFC server program does have to start on a remote host, then make sure that the path and file name of the external library are also valid on the remote host. (The location of the library is specified in the gateway's profile parameter `snc/gssapi_lib` and sent to the external program on the remote host. This path and file name must be valid on the remote host.)

4.3.8 RFC: TCP/IP Connection - Start an External Program over SAPgui

An external program started over SAPgui is started by a user's SAPgui on the workstation where the user has logged on.

For an RFC call that uses a TCP/IP connection to start an external program over SAPgui, the SAP System is the initiator of the communication and the external program is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM59. See *Chapter 4.3.1: Maintaining RFC Destinations and their SNC Options Using Transaction SM59*. The SNC partner name is automatically taken from the SAPgui connection.

An RFC connection to start a program over SAPgui is only protected with SNC if the respective SAPgui also uses SNC protection. This is the only way to make sure that the external program can access the necessary SNC environment (for example, the external library or the logon to the external security product).

Acceptor (external program)

You do not need to specify any additional SNC options for external programs that start over SAPgui. The programs retrieve the SNC information that they need as follows:

- SNC mode and quality of protection

  The SNC mode (active or inactive) for the connection and the quality of protection are defined in transaction SM59 for the initiator and are automatically sent to the program to be started, a part over the command line and a part over messaging from the SNC layer.

- Name and location of the external library

  The external program finds the name and location of the external library (`SNC_LIB`) in the SAPgui parameters.

- SNC name for the external program

  The SNC name for the external program is taken from the SAPgui connection.

4.3.9 RFC: TCP/IP Connection - Registered Program

For an RFC call that uses a TCP/IP connection to call a registered program, the SAP System is the initiator of the communication and the registered program is the acceptor.

Prior to Releases 3.1 and 4.0A, SAP Systems do not support SNC-protected RFC calls to registered programs over TCP/IP connections. In addition, to be able to use SNC protection, a registered program must be linked with an `rfclib` of at least Release 4.5A. It can, however, communicate with a SAP System Release 4.0A/B via a 4.0A/B gateway.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM59. See *Chapter 4.3.1: Maintaining RFC Destinations and their SNC Options Using Transaction SM59*.

Acceptor (registered program)

To apply SNC protection to registered programs that communicate with SAP Systems using RFC, you need to specify the SNC options in either the `saprfc.ini` file or using the program interface in `rfclib`. This section describes how to specify the information in `saprfc.ini`. For more information about using `rfclib`, see *Chapter 4.9:C Program Interfaces*.)

Prerequisites

You have to provide or install accepting credentials for the RFC server program. (The procedure for installing credentials depends on the security product that you use.)

Procedure

Set the SNC parameters in `saprfc.ini` as shown in Table 4-4:

Table 4-4: SNC Parameters for RFC from SAP Systems to Start a Registered Program

Parameter	Description	Required or optional	Permitted Values	Default
`SNC_LIB`	Path and file name of the gssapi library	Required	String value	None
`SNC_MODE`	SNC activation indicator	Required	0, 1 0=SNC disabled 1=SNC activated	None
`SNC_QOP`	Quality of protection (protection level)	Optional	1,2,3,8,9	3
`SNC_MYNAME`	SNC name of the RFC server program	Optional	String value	The SNC name contained in the RFC destination's SNC options.

You can use the parameter SNC_MYNAME to locally define the name that corresponds to the credentials for the RFC server program. If you do, then make sure that this SNC name corresponds to the SNC name as defined in the SNC options (SNC partner name) for the RFC destination for this server program. If you do not locally define SNC_MYNAME, then the registered program uses the SNC name defined in the RFC destination.

Example destination in the `saprfc.ini` file:

```
DEST=Q40
TYPE=R
PROGID=p22124.srfcserv
GWHOST=hs0017
GWSERV=sapgw01
SNC_MODE=1
SNC_MYNAME=p:CN=testuser, OU=TEST01, O=SAP, C=DE
SNC_LIB=I:\secude\LIB\secude.dll
```

Using SNC with Registered Programs

You can only enter one SNC partner name when you enter the SNC options for RFC destinations. Therefore, if two or more programs have the same registered program ID, they must also use the same credentials. This is generally not a problem if the programs are started on the same computer.

However, starting registered programs on different computers is only possible if the same credentials can be used on the different computers. Whether or not this is supported depends entirely on the security product used. Normally, it is **not supported** and **not recommended**!

Gateway Operations

See *Chapter 3.3: Profile Parameter Settings on the Gateway* for information pertaining to SNC with gateway operations.

4.3.10 Remote Logon Using Transaction SM51

When logging on to another application server within a single SAP System using transaction SM51, the system establishes the connection using an internal destination. The connection is automatically SNC-protected if the profile parameter `snc/r3int_rfc_secure` = 1 (apply SNC to internal RFCs).

Keep in mind that we do not recommend using SNC protection for internal RFCs.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the above description is only applicable as of Release 4.0.

4.3.11 Remote Logon Using Transaction SM59

SNC-protected remote logons using transaction SM59 are **not** supported in Release 4.0A.

If a remote logon is attempted to a destination where SNC has been activated, nothing happens! (There is also no error message.)

4.3.12 Special Destinations

The following information applies to SNC protection when using the special RFC destinations BACK and NONE.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Destination BACK

When a function module establishes an RFC call using the destination BACK, the return connection is automatically protected with SNC if the original connection was SNC-protected. The system does not set up a new connection for the BACK destination; it uses the original connection for the return connection.

Destination NONE

The destination NONE is a special internal destination and is handled in the same way as other internal destinations. If you apply SNC protection to internal connections, then connections that use the destination NONE will also use SNC protection. (See the profile parameter `snc/r3int_rfc_secure`.)

4.3.13 Destinations without RFCDES Entry

Destinations without an RFCDES entry cannot use SNC protection.

4.3.14 RFC Groups

RFC groups combine the application servers of a single SAP System into a group. When you use RFC calls to groups (CALL FUNCTION ... DESTINATION IN GROUP ...), the application server is selected at the time of the call. Currently, you cannot apply SNC protection for calls to RFC groups.

RFC groups are internal destinations, and therefore you do not need to protect them with SNC. You can provide protection for internal destinations by isolating your local network and protecting it with a firewall. See *Chapter 2.6: Recommendations.*

4.4 Configuring SNC Options: Using CPIC from SAP Systems

To use SNC with CPIC calls from SAP Systems, you must configure the SNC options for each CPIC destination individually. You can either use transaction SM54 or SM30 (table TXCOMSECU). In this chapter, we describe how to configure the SNC options using transaction SM54.

Transaction SM54 distinguishes the following types of CPIC destinations (depending on the communication partner):

- TYPE = C: R/2 connections
- TYPE = I: R/3 connections
- TYPE = E: Connections to external programs that are started over a gateway
- TYPE = R: Connections to registered external programs

Maintaining SNC options for the initiator (SAP System) is similar for all of the categories and is described in the following section *4.4.1: Maintaining CPIC Destinations and their SNC Options Using Transaction SM54.* The specifics, along with the options to set on the accepting side, are described in the sections *4.4.2 - 4.4.5*.

4.4.1 Maintaining CPIC Destinations and their SNC Options Using Transaction SM54

Use transaction SM54 to configure CPIC destinations for SNC protection.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

When maintaining the SNC options for RFC destinations using transaction SM59, you specify the following SNC information:

- SNC mode for the connection (active or inactive)
- Quality of protection (QoP)
- SNC partner name

The other SNC-relevant settings (the application server's SNC name, the location of the external library, the maximum quality of protection, and the default quality of protection) are applied as defined in the application server's instance profile (see *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server).*

Prerequisites

- SNC is activated on the application server.
- The CPIC destination has been defined.

Procedure

From the *Maintain Table TXCOM* screen (transaction SM54; see Figure 4-6):

1. Place the cursor on the destination application server and choose *XCOM entry* → *Change*.

   The *Change XCOM Entry* screen appears (see Figure 4-7).

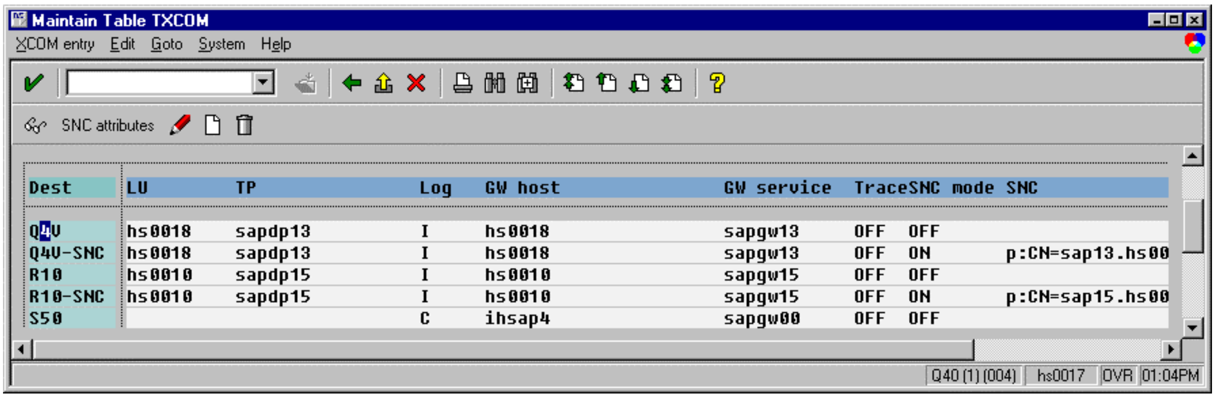
2. To activate SNC for the CPIC destination, enter **ON** in the *SNC Mode* field. (Enter **OFF** to deactivate SNC).

3. Choose *SNC attributes*.

   The *Change View "SNC extension": Details* screen appears (see Figure 4-8).

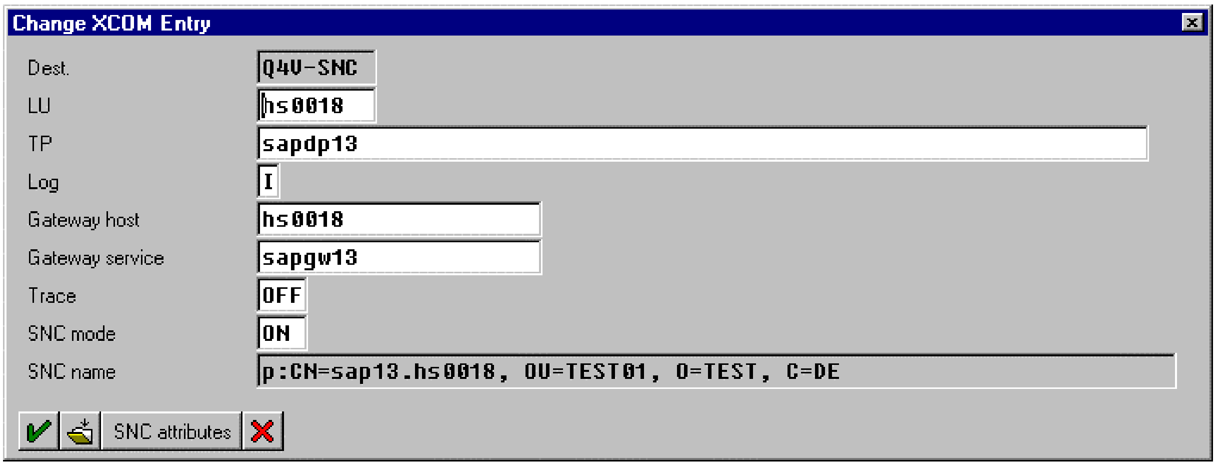
4. Enter the quality of protection in the *QOP* field and the SNC name of the communication partner in the *SNC name* field.

5. Save the data.



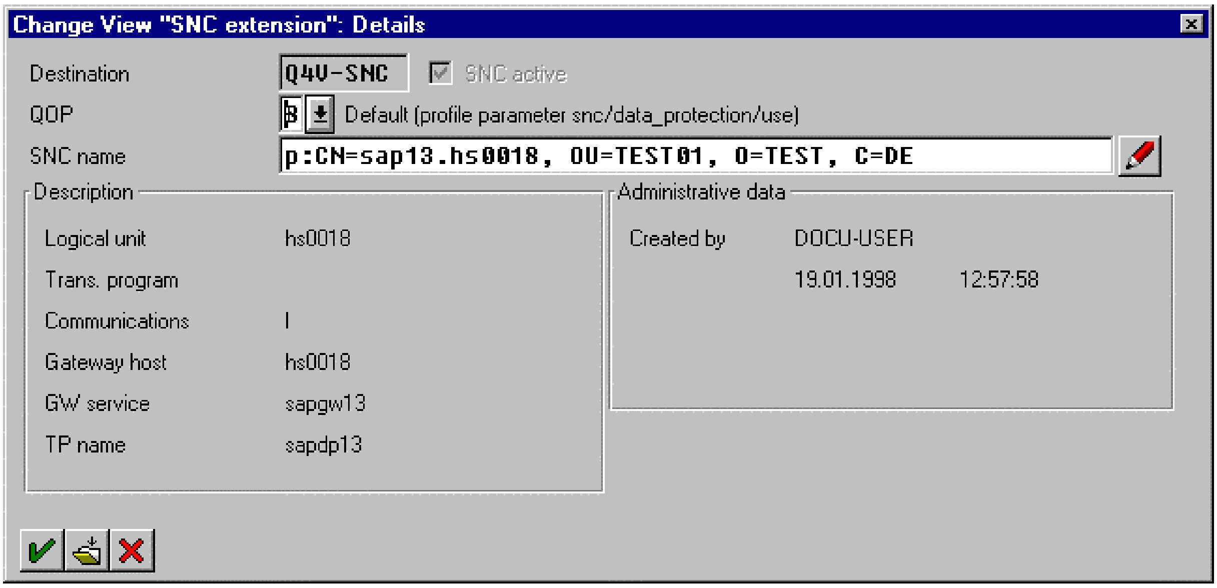
Dest	LU	TP	Log	GW host	GW service	Trace	SNC mode	SNC
Q4V	hs0018	sapdp13	I	hs0018	sapgw13	OFF	OFF	
Q4V-SNC	hs0018	sapdp13	I	hs0018	sapgw13	OFF	ON	p:CN=sap13.hs00
R10	hs0010	sapdp15	I	hs0010	sapgw15	OFF	OFF	
R10-SNC	hs0010	sapdp15	I	hs0010	sapgw15	OFF	ON	p:CN=sap15.hs00
S50			C	ihsap4	sapgw00	OFF	OFF	

Figure 4-6: Maintaining SNC Options for CPIC Destinations (SM54)



Dest.	Q4V-SNC
LU	hs0018
TP	sapdp13
Log	I
Gateway host	hs0018
Gateway service	sapgw13
Trace	OFF
SNC mode	ON
SNC name	p:CN=sap13.hs0018, OU=TEST01, O=TEST, C=DE

Figure 4-7: Maintaining SNC Mode for CPIC Destinations



Change View "SNC extension": Details

Destination	Q4V-SNC ☑ SNC active
QOP	8 Default (profile parameter snc/data_protection/use)
SNC name	p:CN=sap13.hs0018, OU=TEST01, O=TEST, C=DE

Description

Logical unit	hs0018
Trans. program	
Communications	I
Gateway host	hs0018
GW service	sapgw13
TP name	sapdp13

Administrative data

Created by	DOCU-USER	
	19.01.1998	12:57:58

Figure 4-8: Maintaining SNC Options for CPIC Destinations

Quality of Protection (QoP)

The following rules apply to the relationship between the QoP entered in the above screen and the QoP that exists in the application server's profile parameter:

- If the CPIC destination's QoP is larger than the level provided by the external security product, then the largest possible QoP is used.
- If the CPIC destination's QoP = 8 (default), then the QoP value from the application server's `snc/data_protection/use` is used.
- If the CPIC destination's QoP = 9 (maximum), then the QoP value from the application server's `snc/data_protection/max` is used.

There are a few differences to these rules in Release 4.0A. They are described in *Appendix D: Special Cases Relevant to Releases 3.1G/H and 4.0A.*

Set the QoP to either 8 (default) or 9 (maximum value).

4.4.2 CPIC: SAP System → R/2 Connection

SNC for CPIC connections to R/2 (type = C) is currently not supported. There are no security products available for mainframes that support the GSS-API or that are implemented in R/2 at this time.

Therefore, you **cannot** activate SNC for connections defined as protocol type = C! Currently, you receive no error message when you activate SNC in the SNC options; however, you receive an error when you attempt to establish such a CPIC connection.

4.4.3 CPIC: SAP System → SAP System

The SNC configuration for CPIC connections to SAP Systems (type = I in TXCOM) is almost identical to that for RFC internal destinations that do not use load balancing (see *Chapter 4.3.3: RFC: SAP System → SAP System*), with the only difference being that you make your entries in the table TXCOMSECU instead of RFCDESSECU.

For the communication path between two SAP Systems when using CPIC, the calling SAP System is the initiator of the communication and the SAP System that is defined as the CPIC destination system is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM54. See *Chapter 4.4.1: Maintaining CPIC Destinations and their SNC Options Using Transaction SM54*. The SNC name to enter in the SNC options is the destination application server's SNC name.

Acceptor (SAP System)

To be able to receive SNC-protected CPICs from other SAP Systems, you need to specify the corresponding systems in the SNC system ACL (table SNCSYSACL).

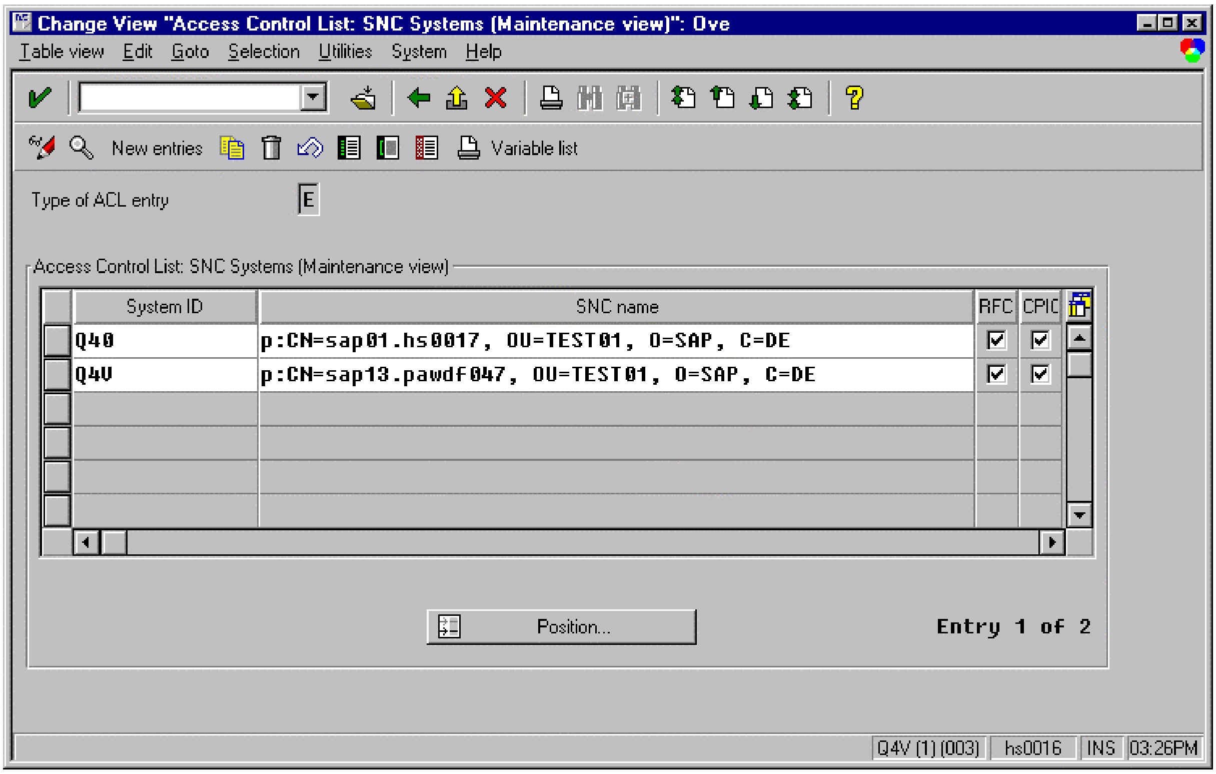
In the accepting SAP System (see also *Chapter 4.3.3: RFC: SAP System → SAP System*):

1. Call transaction SNC0 to maintain entries in the SNC system ACL (table SNCSYSACL; see Figure 4-9).
2. Create an entry **for each application server** from other SAP Systems that needs CPIC access to this SAP System. To create an entry, choose *Edit → New entries*; to modify an existing one, choose *Goto → Details*.

   If you have multiple application servers in a remote SAP System that use different credentials (different SNC names), you need to make an entry for **each** application server in the table SNCSYSACL.

   The table maintenance screen appears.

3. Enter the application server's SNC name in the *SNC name* field.
4. If you have not already done so, activate the *Entry for CPIC activated* indicator.
5. If RFC connections are also to be accepted for this connection, then also activate the *Entry for RFC activated* indicator.
6. If you activate RFCs for the destination, then enter the system ID of the initiating SAP System in the *System ID* field. You do not need to make an entry in this field for CPIC connections.
7. Save the data.



Type of ACL entry: E

Access Control List: SNC Systems (Maintenance view)

System ID	SNC name	RFC	CPIC
Q40	p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE	☑	☑
Q4V	p:CN=sap13.pawdf047, OU=TEST01, O=SAP, C=DE	☑	☑

Entry 1 of 2

Figure 4-9: SNC Entries in the Access Control List for CPICs from SAP Systems

Note the following:

- The entries that you make at this time are saved as external entries (type = E).
- In addition, you need to specify whether the accepting SAP System should accept CPICs that do not use SNC protection. To allow non-protected CPIC connections, set the profile parameter `snc/accept_insecure_cpic` to the value "1" (see *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server*).
- If CPICs are to occur within a single SAP System or on a single application server, then you also have to make an entry for the destination in table SNCSYSACL.

User Authentication

The SAP System performs the user authentication for CPIC connections with SNC in the same manner as for those without SNC. The user and password are always checked for authenticity.

4.4.4 CPIC: Start an External Program over a Gateway

The SNC configuration for CPIC connections to external programs over a gateway (type = E in table TXCOM) is almost identical to that for RFC external programs on an explicit host (see *Chapter 4.3.7: RFC: TCP/IP Connection - Start an External Program on an Explicit Host*). In both cases, the program is started over a gateway and the program uses the environment from the gateway to obtain its security information.

For a CPIC call that starts an external program over a gateway, the calling SAP System is the initiator of the communication and the external program is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM54. See *Chapter 4.4.1: Maintaining CPIC Destinations and their SNC Options Using Transaction SM54*.

Acceptor (external program)

The SNC options as entered in transaction SM54 for the initiator are automatically sent to the program to be started. These options include the SNC mode (active or inactive), the SNC name for the external program (SNC partner name), and the quality of protection.

To specify the path and file name of the external library, the gateway that starts the external program sends the value of its own profile parameter `snc/gssapi_lib` to the external program as a command line parameter. (The command line parameter value overrides the `SNC_LIB` environment variable.)

Gateway Operations

See *Chapter 3.3: Profile Parameter Settings on the Gateway* for information pertaining to SNC with gateway operations.

In addition, note the following:

- Make sure that SNC is activated for the gateway (`snc/enable` = 1) and that the path and file name of the external library are contained in the profile parameter `snc/gssapi_lib`.
- Normally, the gateway will not start external programs without using SNC protection. To enable the starting of external programs without using SNC, set the gateway's parameter `snc/permit_insecure_start` to the value "1".
- When using SNC, we recommend having the gateway start the external programs locally and not on remote hosts. Disable the starting of programs on remote hosts as described in *Chapter 3.3: Profile Parameter Settings on the Gateway*.

The gateway uses the common Berkeley remote shell (`rsh` or `remsh`) to start programs on remote hosts. The Berkeley remote shell performs only a simple authentication based on the IP address and cannot protect the TCP datastream that it uses. Therefore, we recommend that you do not use the starting of programs on remote hosts when using SNC.

- However, if the external program does have to start on a remote host, then make sure that the path and file name of the external library is also valid on the remote host. (The location of the library is specified in the gateway's profile parameter `snc/gssapi_lib` and sent to the external program on the remote host.)

4.4.5 CPIC: Registered Program

CPIC registered programs are saved in the table TXCOM with type = R. For a CPIC call that starts a registered program, the calling SAP System is the initiator of the communication and the registered program is the acceptor.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following description is only applicable as of Release 4.0.

Initiator (SAP System)

To specify the SNC options for the initiator (SAP System), use transaction SM54. See *Chapter 4.4.1: Maintaining CPIC Destinations and their SNC Options Using Transaction SM54.*

Acceptor (registered program)

The SNC options as entered in SM54 for the initiator are automatically sent to the program to be started. These options include the SNC mode (active or inactive), the SNC name for the external program (SNC partner name), and the quality of protection.

To specify the path and file name of the external library, the gateway that starts the external program sends the value of its own profile parameter `snc/gssapi_lib` to the external program as a command line parameter. (The command line parameter value overrides the `SNC_LIB` environment variable.)

Because the registered program needs access to the external library, and the gateway provides its location, you can only use SNC protection for registered programs that are started on the computer where the gateway is located.

Gateway Operations

For information about using SNC with gateway operations, see *Chapter 3.3: Profile Parameter Settings on the Gateway*.

4.5 Configuring SNC Options: Printing

You can also apply SNC protection to data being printed. This applies to both printing on the frontend computer (access method = F) and printing using SAPlpd (access method = S).

4.5.1 Printing on a Frontend Computer

Printing on a frontend computer is automatically protected with SNC if the SAPgui connection is SNC-protected. For Releases up to and including 4.0B, you do have to make the following setting:

From the *Spool Administration: Initial Screen* (transaction SPAD):

1. Choose *Settings* → *Spool System*.
2. Enter **`SAPGUI`** in the *RFC destination for frontend printout* field.
3. Save the data.

4.5.2 Printing Using SAPlpd

When printing using SAPlpd (printing with access method = S), the SAP System spool work process is the initiator of the communication and the SAPlpd program on the printer server is the acceptor.

Initiator (SAP System)

To configure SAPlpd to use SNC protection, use the spool administration (transaction SPAD).

Prerequisites

- SNC must be activated on the application server (`snc/enable` = 1).
- The printer must use the access method type = S (Print on LPDHOST via SAP protocol).

Procedure

From the *Spool Administration: Initial Screen* (transaction SPAD):

1. Choose *Configuration* → *Output devices*.

   A list of output devices appears.
2. To maintain an existing device, select the output device and choose *Output device* → *Choose*; to create a new device, choose *Output device* → *Create*.

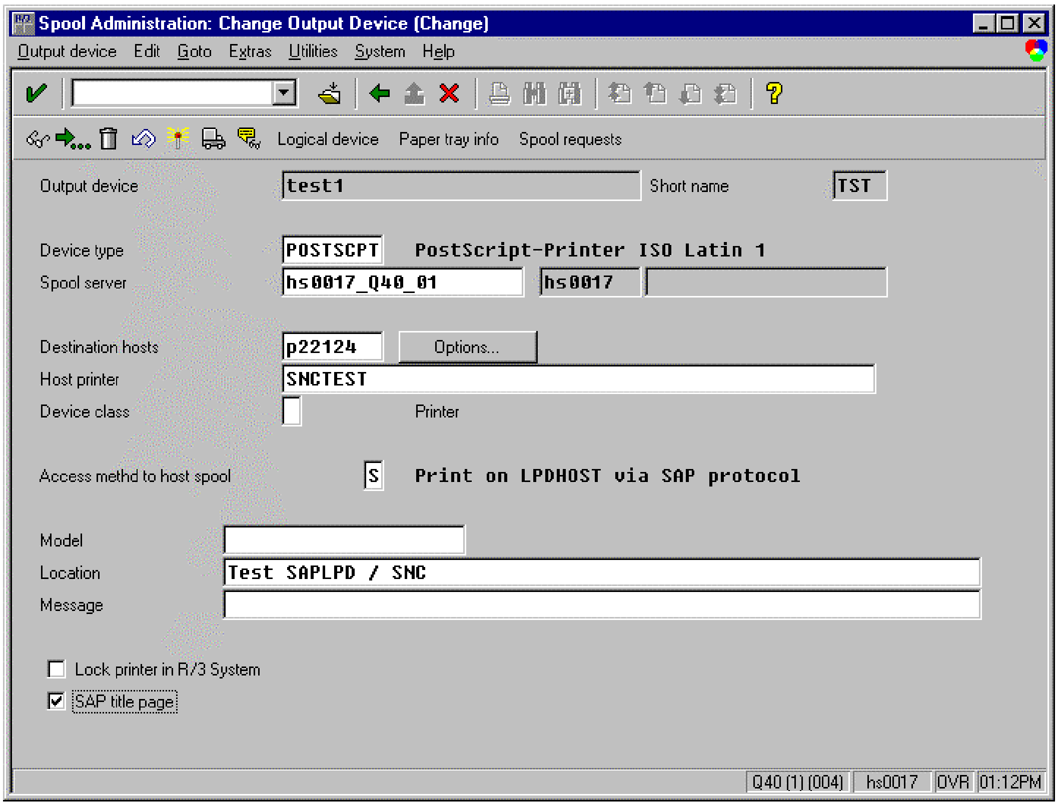
   The maintenance screen for the device appears (see Figure 4-10).
3. Enter the data.

   To be able to use SNC for the connection, enter the value **`S`** in the *Access method to host spool* field.
4. Choose *Next screen* ➔.

   The second maintenance screen appears (see Figure 4-11).

5. Select the *No longer ask for print requests in host spool* indicator.
6. Enter the rest of the printer data.
7. Choose *Next screen*.

   The third spool maintenance screen appears (see Figure 4-12).
8. To activate SNC and specify the level of protection, select the appropriate indicator in the *Security of connection to SAPlpd* group. SNC is only activated if you select *Authentication of the partner* (equivalent to QoP = 1), *Authentication and signing* (equivalent to QoP = 2), *or Authentication and security for privacy* (equivalent to QoP = 3).
9. Select the *Optional* indicator if SNC protection is not mandatory for the communication. (For a variety of reasons, it may not be possible for all communications using SAPlpd to be SNC-protected.) If only SNC-protected communications are to be accepted, then select *Mandatory*.
10. Enter the SNC name of the SAPlpd in the *Identity of the remote SAPlpd for the security system* field.
11. Save the data.



Output device: test1
Short name: TST

Device type: POSTSCPT PostScript-Printer ISO Latin 1

Spool server: hs0017_Q40_01 hs0017

Destination hosts: p22124

Host printer: SNCTEST

Device class: Printer

Access methd to host spool: S Print on LPDHOST via SAP protocol

Model:

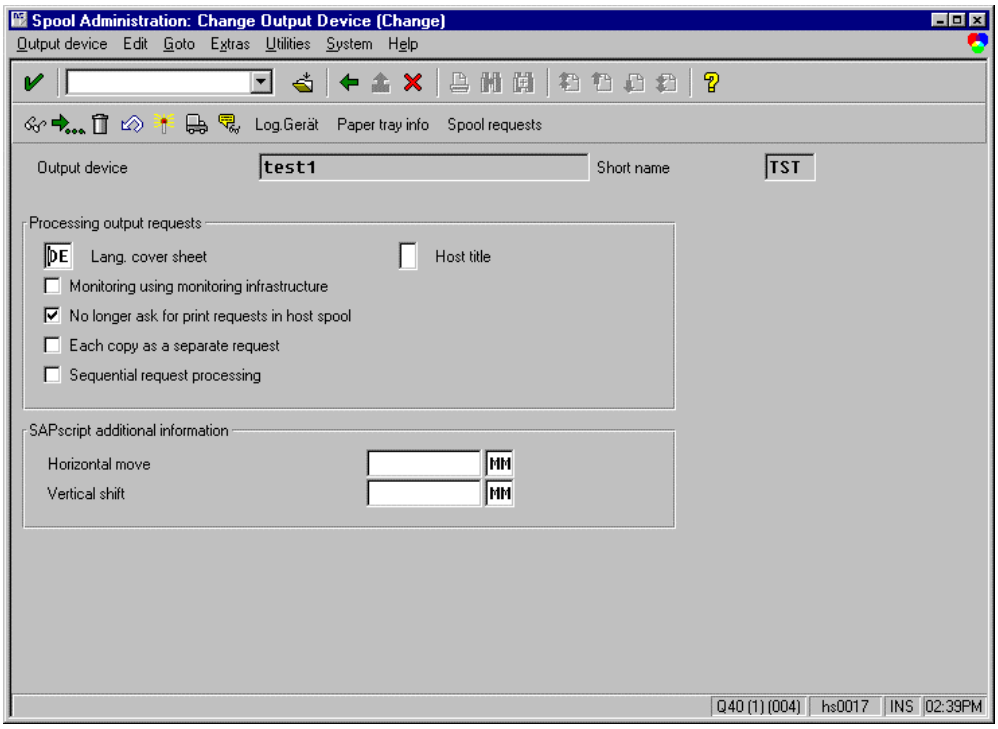
Location: Test SAPLPD / SNC

Message:

☐ Lock printer in R/3 System

☑ SAP title page

Figure 4-10: Spool Administration: Access Method Type S


Spool Administration: Change Output Device (Change)
Output device Edit Goto Extras Utilities System Help
Log.Gerät Paper tray info Spool requests
Q40 (1) (004) hs0017 INS 02:39PM

Output device test1 Short name TST

Processing output requests

DE Lang. cover sheet □ Host title

□ Monitoring using monitoring infrastructure

☑ No longer ask for print requests in host spool

□ Each copy as a separate request

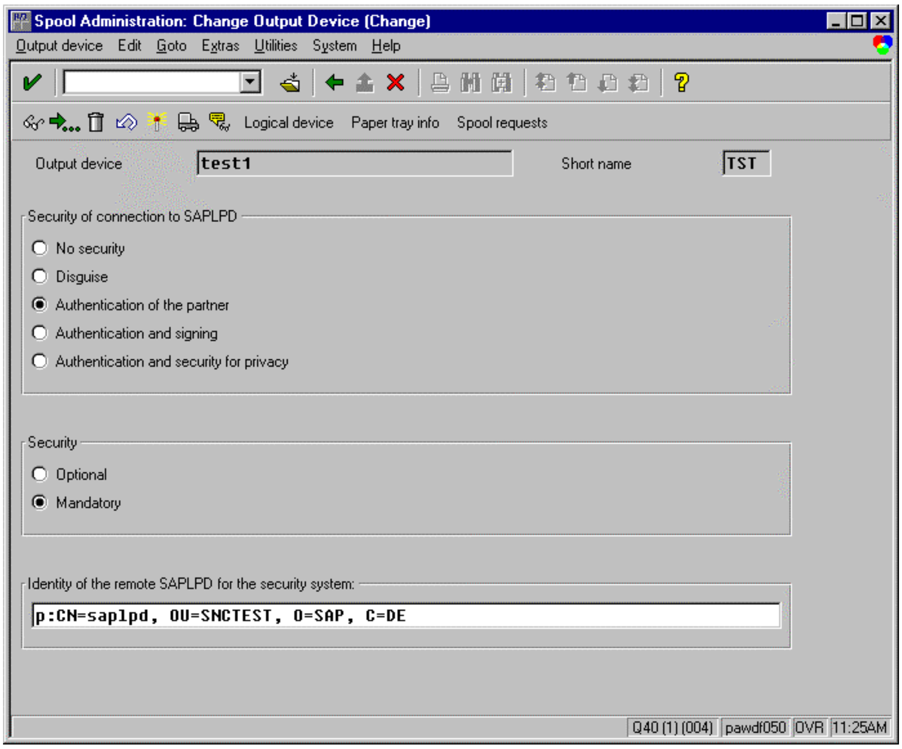
□ Sequential request processing

SAPscript additional information

Horizontal move MM

Vertical shift MM

Figure 4-11: Spool Administration: No Longer Ask for Print Requests in Host Spool


Spool Administration: Change Output Device (Change)
Output device Edit Goto Extras Utilities System Help
Logical device Paper tray info Spool requests
Q40 (1) (004) pawdf050 OVR 11:25AM

Output device test1 Short name TST

Security of connection to SAPLPD

○ No security

○ Disguise

● Authentication of the partner

○ Authentication and signing

○ Authentication and security for privacy

Security

○ Optional

● Mandatory

Identity of the remote SAPLPD for the security system:

p:CN=saplpd, OU=SNCTEST, O=SAP, C=DE

Figure 4-12: Spool Administration: SNC Options

Acceptor (SAPlpd)

On the accepting side (SAPlpd), you need to specify the SNC parameters in the `win.ini` file. You also need to specify additional options after starting SAPlpd.

Specifying SNC parameters in `win.ini`

Prerequisites

You want to protect the communication between the SAP System and SAPlpd with SNC. The following parameters are not necessary if you do not want to use SNC.

Procedure

1. To activate SNC, create a section called `[snc]` in the `win.ini` file.
2. Set the SNC parameters shown in Table 4-5 in the `win.ini` file.

Table 4-5: SNC Parameters for SAPlpd

Parameter	Description	Required or optional	Permitted Values	Default
`gssapi_lib`	Path and file name of the gssapi library	Required	String value	None
`enable`	SNC activation indicator	Required	0, 1 0=SNC disabled 1=SNC activated	None
`identity/lpd`	SNC name of SAPlpd	Required	String value	None

Example destination in the `win.ini` file:

```
[snc]
enable=1
gssapi_lib=C:\SECUDE\LIB\SECUDE.DLL
identity/lpd=p:CN=saplpd.p22124, OU=TEST01, O=SAP, C=DE
```

Specifying Additional SNC Options for SAPlpd

Prerequisites

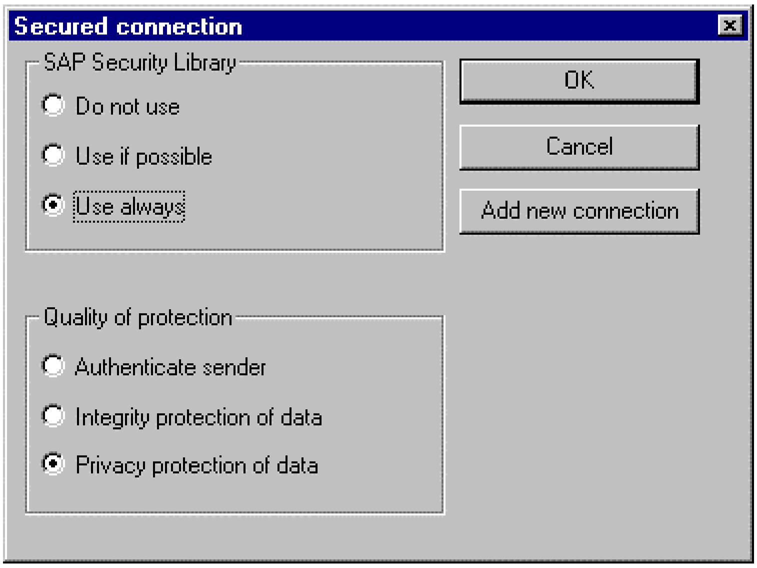
You have started SAPlpd.

Procedure

From the *Saplpd.log -SAPLPD* dialog box:

1. Choose *Options* → *Secured Connection*.

   The *Secured connections* screen appears (see Figure 4-13).



Secured connection

SAP Security Library

○ Do not use

○ Use if possible

● Use always

Quality of protection

○ Authenticate sender

○ Integrity protection of data

● Privacy protection of data

Figure 4-13: Spool Administration: Additional SNC Options

2. Choose the appropriate option from the *SAP Security Library* group. This setting must correlate with the *Security* setting in the SAP System (*Mandatory* or *Optional*). The options have the following meanings:

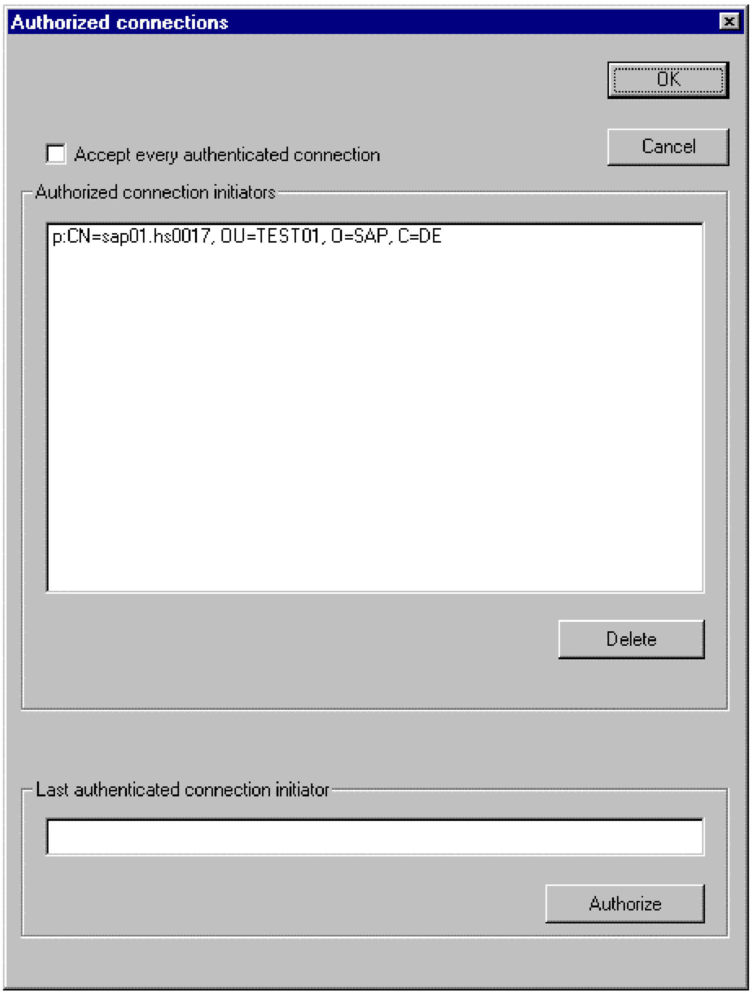
• *Do not use*	All communications are insecure
• *Use if possible*	SNC-protection depends on the initiator
• *Use always*	Accept only SNC-protected connections

3. Set the *Quality of protection* (QoP) by choosing the appropriate option. This setting **must be the same as** the quality of protection level set in the SAP System. The options have the following meanings:

• *Authenticate sender*	QoP = 1:	Authentication only
• *Integrity protection of data*	QoP = 2:	Authentication and integrity protection
• *Privacy protection of data*	QoP = 3:	Authentication, integrity protection, and privacy protection

4. Choose *Add new connection* to specify the partners SAPlpd should accept.

   The *Authorized connections* screen appears (see Figure 4-14).



□ Accept every authenticated connection

Authorized connection initiators

p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE

Last authenticated connection initiator

Figure 4-14: Spool Administration: Authorized Communication Partners for SAPlpd

5. Either select *Accept every authenticated connection* to accept all connections or create a list of the individual partners to accept.

   To add partner names to the list:

   a) Enter the partner's SNC name in the *Last authenticated connection initiator* field.

   b) Choose *Authorize*.

      If you choose to accept all connections, then the name of the last accepted partner automatically appears in the *Last authenticated connection initiator* field. You can then add it to the list.

6. Choose *OK*.

Result

The configuration is automatically saved in the `win.ini` file.

4.6 Configuring SNC Options: SAProuter ←→ SAProuter

The SAProuter is a program that acts as an intermediate location in the network between SAP Systems or SAP programs where access is controlled before data is sent further along the communication path.

Connections can also be established between SAP components over several SAProuters. You can then secure connections between adjacent SAProuters using SNC. A typical example is shown in Figure 4-15.

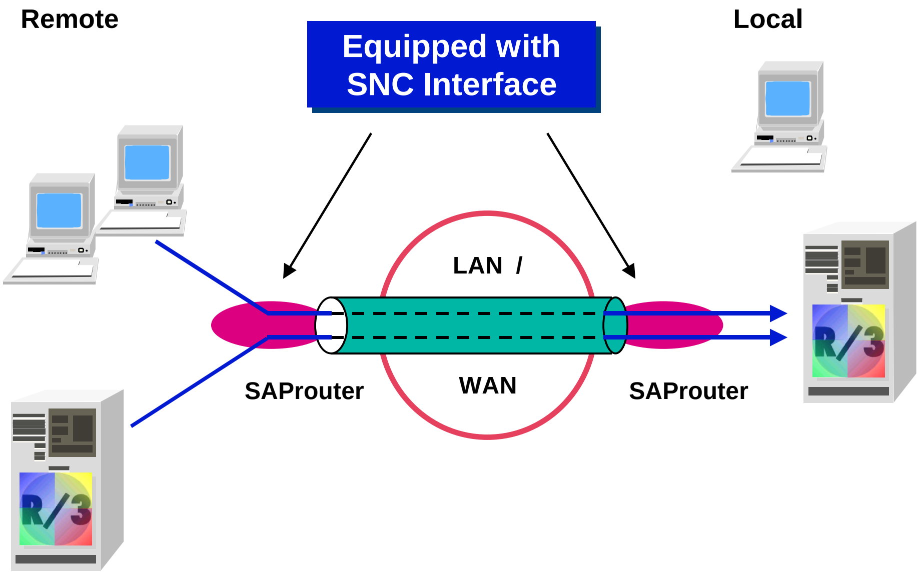


Figure 4-15: SNC Communication Between SAProuters

The connection between the adjacent SAProuters is protected using SNC. The SAProuters authenticate each other and encrypt the exchanged messages. In this way, you can establish a secure "tunnel" for communications between components that may not be able to use SNC themselves (for example, components belonging to an earlier release).

A single SAProuter can be both the initiator and acceptor for an SNC-protected connection.

For a detailed description on the SAProuter, see the online documentation*BC SAProuter* [7]. In this document, we only describe the aspects that relate to SNC.

To establish SNC-protected connections between two SAProuters:

- You must establish an SNC environment for both SAProuters.
- You must activate SNC for the connection in the SAProuter's route permission table.

Establishing the SNC Environment

Perform the following steps to establish the SNC environment for each SAProuter:

1. On each SAProuter host, make sure that the environment variable `SNC_LIB` contains the path and file name of the external library.
2. Start the SAProuter with the option `-K <snc-name>`, where `<snc-name>` is the SNC name of the SAProuter being started.

The SAProuter then loads the external library and initializes the SNC environment.

Configuring SNC in the Route Permission Table

There are two types of entries that you need to make in the SAProuter route permission table:

- `KT` (Key-Target) entries

  A Key-Target entry specifies that the designated SAProuter → SAProuter connection should use SNC.

- `KP-` / `KD-` / `KS-` entries

  These entries are similar to the normal `P-` / `D-` / `S-` entries, but are used for SNC connections instead of standard connections. They specify the hosts and services that are or are not allowed to communicate with one another. As with normal `P-` / `D-` / `S-` entries, you can also specify a password for the connection.

  You must pay attention to the order of the entries in the route permission table. For incoming connections, the SAProuter applies the first matching entry it finds in the route permission table. If a matching `P-` / `D-` / `S-` entry precedes an SNC entry, the SAProuter ignores the SNC entry. See the example on the following page.

KT Entries

To specify a KT entry, enter a line in the SAProuter's route permission table using the following syntax:

```
KT <SNC_partnername> <dest-host> <dest-serv>
```

Where:

- SNC should be activated for connections to `<dest-host> <dest-serv>`.
- `<SNC_partnername>` is the SNC name of the communication partner.
- `<dest-host>` is the name of the host (either the symbolic name or the IP address).
- `<dest-serv>` is the name of the service (either the symbolic name or the port number).

A wildcard entry (*) for `<dest-host>` or `<dest-serv>` is not practical because the SNC partner name refers to a distinct partner.

To avoid conflicting entries, make `K-` entries before any normal `P-` / `D-` / `S-` entries.

KP- / KD- / KS- Entries

You must also enter `KP-` / `KD-` / `KS-` entries in the route permission table instead of `P-` / `D-` / `S-` entries for the SNC connections. These entries have the same meanings as the `P-` / `D-` / `S-` entries, except that the name of the source host or IP address is replaced with the SNC name of the source host. They have the following syntax:

```
     K<D/P/S> "<SNCname_of_source-host>" <dest-host> <dest-serv> <Password>
```

The SAProuter establishes (`KT`, `KS`) or denies (`KD`) a connection if the values received from the connection request match those in the above mentioned route permission table entries.

Quality of Protection (QoP)

When using SNC protection between SAProuters, the maximum available quality of protection is always applied.

Accepting the Incoming Connection

The SAProuter accepts an incoming connection if it finds a corresponding entry in it's route permission table. For normal incoming connections (that do not use SNC protection), it identifies the communication partner using the source host (IP address) and the destination (host and service). However, for SNC-protected connections coming from a SAProuter, it uses the source SAProuter's SNC name for identification.

Sample SAProuter Configurations when Using SNC

Two SAProuters, one on `host1`, the other on `host2`, are to communicate with another using SNC protection. The SAProuter on `host2` should accept only SNC-protected connections from `host1` that are directed to a dispatcher or gateway with a system number 00.

SNC names of SAProuters on `host1` and `host2`:

SNC name on `host1`: `"p:CN=saprout1, OU=TEST01, O=SAP, C=DE"`
SNC name on `host2`: `"p:CN=saprout2, OU=TEST01, O=SAP, C=DE"`

Starting SAProuter on `host1`:

The following entry starts the SAProuter on `host1`:

```
saprouter -r -K "p:CN=saprout1, OU=TEST01, O=SAP, C=DE" &
```

Route Permission Table on `host1`:

The route permission table on `host1` contains the following entries:

```
# Initiating SNC for all connections to host2 :
KT = "p:CN=saprout2, OU=TEST01, O=SAP, C=DE"   host2   *
# Accepting all connections
P     *     *     *
```

Starting SAProuter on `host2`:

The following entry starts SAProuter on `host2`:

```
saprouter -r -K "p:CN=saprout2, OU=TEST01, O=SAP, C=DE" &
```

Route Permission Table on `host2`:

The route permission table on `host2` contains the following entries:

```
# accept incoming connections from SAProuter1
#     with destination sapdp00 on any host
KP "p:CN=saprout1, OU=TEST01, O=SAP, C=DE" *     sapdp00
# accept incoming connections from SAProuter1
#     with destination sapgw00 on any host
KP "p:CN=saprout1, OU=TEST01, O=SAP, C=DE" *     sapgw00
```

As previously mentioned, you must pay attention to the order of the entries in the route permission table. The SAProuter applies the first matching entry it finds. In the following example, the SAProuter will not accept the SNC-protected connection request from `host1` to `host2` because of the first entry.

```
D  host1     *     *
KP "p:CN=saprout1, OU=TEST01, O=SAP, C=DE"  *     sapdp00
```

In the following example, the second line is unnecessary because the first line allows all connections from `host1`. Therefore, the second line does not enforce SNC protection for connections to `sapdp00`.

```
P  host1     *     *
KP "p:CN=saprout1, OU=TEST01, O=SAP, C=DE"  *     sapdp00
```

4.7 Configuring SNC Options: SAP Internet Transaction Server → SAP System

As of Release 4.5B, you can also apply SNC protection to the communication between the SAP Internet Transaction Server (ITS) components (WGate and AGate) and SAP Systems.

The following components are involved:

- WGate
- AGate
- SAP System application server

The security product you use for SNC may require you to set certain SNC options in environment variables or Windows NT Registry keys. Note that if you have installed the WGate and AGate on a single host, then you **cannot** use global environment variables or Registry keys for such settings.

In this case, you can use the following Windows NT Registry keys to specify different variable values for each component:

```
HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\
Programs\[AGate|MManager|WGate]\environment\<variable>
```

In this document, we describe only the aspects involved with configuring the SAP System and ITS for using SNC. For more information the ITS, see the SAP library (R/3 library) online documentation *Internet Transaction Server* [5] and the *SAP@Web Installation Guide* [2].

We describe the configuration for each of the components in the sections that follow.

WGate

Prerequisites

- The WGate component of the ITS has been installed on the Web server.
- The security product has been installed on the WGate host.
- You know the SNC names of the WGate and the AGate.

Procedure

1. Specify the location of the external library in the environment variable `SNC_LIB` on the WGate host.
2. To specify that SNC should be applied to the connection, and to specify the SNC names of the communication partners (WGate and AGate), enter the values shown in Table 4-6 in the WGate's configuration.

   If you use the ITS Administration Tool, make the entries under *Security → Network Security*. Otherwise, make the entries in the Windows NT Registry key:

   ```
   KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Connects
   ```

Table 4-6: SNC Parameters for the WGate

Parameter	Value	Comment
`Type`	2	Use NISNC based connection (SAP protocol NI plus SNC)
`SncNameWGate`	SNC name of the WGate	
`SncNameAGate`	SNC name of the AGate and ITS Manager	The AGate and ITS Manager share the same security environment and therefore the same SNC name

3. Perform any product-specific tasks. For example, you may have to establish a security environment or issue credentials for the WGate.
4. Restart the Web server.
5. Check the ITS trace file `WGate.trc` for errors. For an example trace file after successful SNC installation, see *Appendix E: SNC Messages.*

AGate

Prerequisites

- The AGate component has been installed on the ITS server.
- The security product has been installed on the AGate host.
- You know the SNC names for the WGate and the SAP System application server.

Procedure

1. Specify the location of the external library.

   Define the location of the external library in the environment variable `SNC_LIB` on the AGate host.

2. Specify the SNC options for the WGate ←→ AGate connection.

   Specify the AGate's SNC options for the connection between the AGate and the WGate by entering the values shown in Table 4-7 in the AGate's configuration.

   If you use the ITS Administration Tool, make the entries under *Security* → *Network Security*. Otherwise, make the entries in the Windows NT Registry key:

   ```
   KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Connects
   ```

Table 4-7: SNC Parameters on the AGate for Communication with the WGate

Parameter	Value	Comment
`Type`	2	Use NISNC based connection (SAP protocol NI plus SNC).
`SncNameAGate`	SNC name of the AGate and ITS Manager	The AGate and ITS Manager share the same security environment and therefore, the same SNC name.
`SncNameWGate`	SNC name of the WGate	

3. Specify the SNC options for the AGate ←→ SAP System connection.

   To define the SNC options for the communication between the AGate and the SAP System application server, enter the SNC options as shown in Table 4-8 in the AGate's service files. You can make the entries either in the global service file `global.srvc` or in the local services files belonging to each Internet Application Component (IAC). An entry in a local service file overrides that in `global.srvc`.

   If you use SNC protection with the ITS, then all of the IACs must communicate with the SAP System using SNC. You cannot operate with a mixed environment. Make sure that all of the IAC service files have access to the SNC parameters.

Table 4-8: SNC Parameters on the AGate for Communication with the SAP System

Parameter	Value	Comment
`~sncNameAGate`	AGate's SNC name	You must specify the AGate's SNC name in one of the following ways: • Registry entry In this case, the AGate uses the same SNC name for the AGate ←→ SAP System connection as with the AGate ←→ WGate connection. • Entry in the global services file In this case, you specify a default SNC name for the AGate for all services, which may differ from the SNC name used in the WGate ←→ AGate connection. • Entry in the local service file In this case, you specify a service-specific SNC name for the AGate.
`~sncNameR3`	Application server's SNC name	This entry is mandatory in either the local service file or in the global service file `global.srvc`. An entry in `global.srvc` specifies a default application server SNC name for all services. An entry in a local service file overrides that in `global.srvc`.
`~sncQoPR3`	Quality of protection level to use	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from the application server's profile parameter `snc/data_protection/max`

   If you support the use of X.509 certificates for logon to SAP Systems via the ITS, then you also have to set the service file parameter `~clientCert` to the value "1" in the local service files for all IACs that support the X.509 certificate logon.

   Note however, we do not describe the complete configuration procedures for using X.509 certificates in this document. For more information, see the document *X.509 Certificate Logon via the ITS* [4].

4. Perform any product-specific tasks. For example, you may have to establish a security environment or issue credentials for the AGate.

5. Restart the ITS Manager.

6. Check the ITS trace file `AGate.trc` and `Mmanager.trc` for errors. For an example trace file after successful SNC installation, see *Appendix E: SNC Messages*.

SAP System Application Server

Prerequisites

- The security product has been installed on the application server.
- You know the SNC names of the AGate and the SAP System application server.

Procedure

1. To enable SNC on the application server, set the SNC profile parameters according to *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server.*
2. Specify the AGate's SNC information in the SNC access control list (table SNCSYSACL, view VSNCSYSACL, type = E).
   a) Enter the *System ID* and the *SNC name* for the AGate.

      The *System ID* field is optional. The SAP System does not need it to identify the AGate; it uses the SNC name. However, you can assign a system ID to the AGate to improve transparency.

   b) Activate the options *Entry for RFC activated* and *Entry for CPIC activated*.

   c) If you use X.509 certificates for logging on to the SAP System via the ITS, then activate the option *Entry for certificates activated*.

   d) Save the data.
3. If you use WebRFC, then you have to create a generic entry in the extended user ACL (table USRACLEXT). This entry allows WebRFC users access to the SAP System using the AGate's SNC-protected connection. For details on maintaining the extended user ACL, see *Chapter 3.6.2: Maintaining SNC Information for Non-Dialog Users*.

   The specifics for this scenario are as follows:

   a) Enter an asterisk (*) in the *User* field.

   b) If you create several entries for the same SNC name, then enter the appropriate sequence number in the *Seq.number* field.

   c) Enter the AGate's SNC name in the *SNC name* field.

   d) Save the data.

      You receive a warning due to the wildcard entry in the *User* field.

4.8 Special Cases

In this chapter, we describe the following special cases:

- *Using Microsoft's NT LAN Manager Security Support Provider for Single Sign-On under Windows NT*
- *Communication with the Message Server*
- *SAPgui Started per RFC*

4.8.1 Using Microsoft's *NT LAN Manager Security Support Provider* for Single Sign-On under Windows NT

SNC generally requires the use of a SAP-certified external security product to provide its protection. However, to integrate SAP Systems into a Single Sign-On environment under Windows NT, you can use Microsoft's *NT LAN Manager Security Support Provider* (NTLMSSP) as the security provider. You can also find information about this scenario in the *R/3 Installation on Windows NT* [3] documentation.

Microsoft's NTLMSSP provides a uni-directional authentication of the initiator (client) to the acceptor (server) only. It does **not** provide mutual authentication, and it does not offer data integrity or data privacy protection for the communication.

Prerequisites

- A complete Windows NT environment is required. The NTLMSSP is not supported under UNIX or other operating system platforms.
- Bi-directional trust is required between the Windows NT domains if you use separate domains for the frontend clients and the SAP System application servers.

For security aspects involved with this scenario, see SAPNet Note 165485 [11].

Activities

So that you can use Microsoft's NTLMSSP as the security provider for Single Sign-On, we provide the dynamic link library `gssapi32.dll`, which offers a GSS-API V2 compliant interface for the NTLMSSP on Win32 platforms.

To use Microsoft's NTLMSSP for Single Sign-On, you need to perform the following tasks:

1. Install the GSS-API V2.
2. Activate SNC on the application server.
3. Maintain users in the SAP System.
4. Configure SNC options for the communication partners (SAPgui and the SAP System).

We describe the details that are specific to this scenario below.

4.8.1.1 Installing the GSS-API V2

To install the GSS-API V2 library, copy the file `gssapi32.dll` from the Kernel CD to your central instance. You can find this file on the Kernel CD in the path:

- Standard: `<CD_DRIVE>:\NT\I386\`
- DEC ALPHA: `<CD_DRIVE>:\NT\ALPHA\`

For the target directory, we suggest using the following path on your main instance:

```
<DRIVE>:\USR\SAP\<SID>\SYS\EXE\RUN
```

4.8.1.2 Activating SNC on the SAP System Application Server

On the SAP System application server, set the SNC parameters as shown in Table 4-9.

The following parameter settings refer to a 4.0B system or higher. If you are using Release 3.1, then you need to adjust the settings accordingly.

Table 4-9: Profile Parameter Settings for Single Sign-On Using Microsoft's NTLMSSP

Parameter	Value
`snc/data_protection/max`	`1`
`snc/data_protection/min`	`1`
`snc/data_protection/use`	`1`
`snc/enable`	`1`

`snc/gssapi_lib`	`<location of gssapi32.dll>\gssapi32.dll`
	For example, if you used our suggestion above, then assign the following value to the profile parameter:
	`<DRIVE>:\USR\SAP\<SID>\SYS\EXE\RUN\gssapi32.dll`

`snc/identity/as`	`p:<DOMAIN_NAME>\<SID>ADM` where `<DOMAIN NAME>` is the Windows NT domain that the user `<SID>ADM` belongs to.

For more information about these and other SNC parameters (for example, `snc/accept_insecure_cpic` or `snc/accept_insecure_gui`), see *Chapter 3.2: Profile Parameter Settings on the SAP System Application Server.*

4.8.1.3 Maintaining Users in the SAP System

Assign SNC names to your users using transaction SU01 as described in *Chapter 3.6.1: Maintaining SNC Information for Dialog Users*.

Define the SNC names as follows:

SNC name = `p:<DOMAIN_NAME>\<NT_USERNAME>`

Where: `<DOMAIN_NAME>` is the Windows NT domain that the user belongs to and `<NT_USERNAME>` is the user's Windows NT logon ID.

If you want to allow certain users access to the SAP System without requiring the use of Single Sign-On, then select *Insecure communication permitted*.

This option, which is available as of Release 4.0, allows you to permit the conventional password-based logon for individual users. To use this option, the profile parameter `snc/accept_insecure_gui` must also be set to the value "U".

4.8.1.4 Configuring SNC Options: SAPgui and SAP System

To configure the communication partners SAPgui and the SAP System, follow the descriptions provided in *Chapter 4.1: Configuring SNC Options: SAPgui → SAP System.* Note the following:

- Define the location of the file `gssapi32.dll` in the Windows NT environment variable `SNC_LIB`.

  For example, if you used our suggestion above, then assign `SNC_LIB` the following values:

  SAP System application server:

  `SNC_LIB=<DRIVE>\usr\sap\<SID>\sys\exe\run\gssapi32.dll`

  Frontend client:

  `SNC_LIB=<DRIVE>:\<SAPgui path>\gssapi32.dll`

  where `<SAPgui path>` is the path name for the SAPgui files (for example `c:\SAPpc\sapgui`).

- Assign the parameter `SNC_PARTNERNAME` (direct start) or *SNC name* (in the SAP Logon *Advanced Options)* the value `p:<DOMAIN_NAME>\<SID>ADM`.

  Where `<DOMAIN_NAME>` is the Windows NT domain that the user `<SID>ADM` belongs to.

- Quality of Protection: *Authentication only* is always applied as the quality of protection level when using the Microsoft NTLMSSP, regardless of the setting defined in the parameter `SNC_QOP`. (The Microsoft NTLMSSP does not support data integrity or data privacy protection.)

4.8.2 Communication with the Message Server

SNC protection for communication with the message server is currently not supported.

4.8.3 SAPgui Started per RFC

If SAPgui is started by an RFC program that uses SNC, it inherits the SNC options from the RFC connection.

4.9 C Program Interfaces

We supply C program interfaces for both external CPIC programs as well as for external RFC programs. These interfaces are described in the following sections.

Release 3.1 does not offer SNC protection for the RFC and CPIC communication protocols. Therefore, the following descriptions are only applicable as of Release 4.0.

4.9.1 Interfaces to External CPIC Programs

The SNC configuration for external CPIC client programs is located in the `sideinfo` file. For CPIC server programs (started or registered), the SNC parameters are passed to the server program from the client (see *Chapter 4.4.4: CPIC: Start an External Program over a Gateway* and *Chapter 4.4.5: CPIC: Registered Program*).

SNC information is available to C programs using the following functions in the SAP CPIC Interface:

Table 4-10: SNC-Relevant CPIC Functions

Function	Description
`SAP_CMSNCMODE`	Returns whether SNC is active or not
`SAP_CMSNCNAME`	Returns the SNC name of the partner in printable form
`SAP_CMACLKEY`	Returns the SNC name of the partner in canonical form ("ACLKEY")
`SAP_CMNAMETOACLKEY`	Converts an SNC name to canonical form
`SAP_CMACLKEYTONAME`	Converts an SNC name from canonical form to printable form

For more information about these functions, see the SAP Library (R/3 Library) under*BC SAP Communication: CPI-C Programmer’s Guide* [8].

4.9.2 Interfaces to External RFC Programs

The SNC configuration for external RFC client programs is located in the `saprfc.ini` file. For an RFC server program (for example, a program started from a gateway), the SNC parameters are passed to the server program from the client. (For information about starting external RFC programs, see *Chapters 4.3.6, 4.3.7, 4.3.8*, and *4.3.9*).

You can also specify the parameters from the RFC interface using the function:

`RfcOpenEx`	Open an RFC connection (SNC parameters are specified in the `connect_param` string)

You can use the following functions to obtain SNC information:

Table 4-11: SNC-Relevant RFC Functions

Function	Description
`RfcOpenEx`	Returns whether SNC is active or not
`RfcSncPartnerName`	Returns the SNC name of the partner printable form)
`RfcSncPartnerAclKey`	Returns the SNC name of the partner in canonical form ("ACLKEY")
`RfcSncNameToAclKey`	Converts an SNC name to canonical form
`RfcSncAclKeyToName`	Converts an SNC name from canonical form to printable form

For more information about these functions, see help file `saprfc.hlp`, which is delivered with the RFC Software Development Kit.

5 FAQs

The following are the most frequently asked questions pertaining to SNC.

- **Does a user who has logged on with SNC protection receive dialog boxes for changing his or her password?**

  No.

- **How can I make my current external CPIC programs capable of using SNC?**

  You must link the programs using the current `cpictlib`. Additionally, update the configuration in the `sideinfo` file to include the SNC parameters.

- **How can I make my current external RFC programs capable of using SNC?**

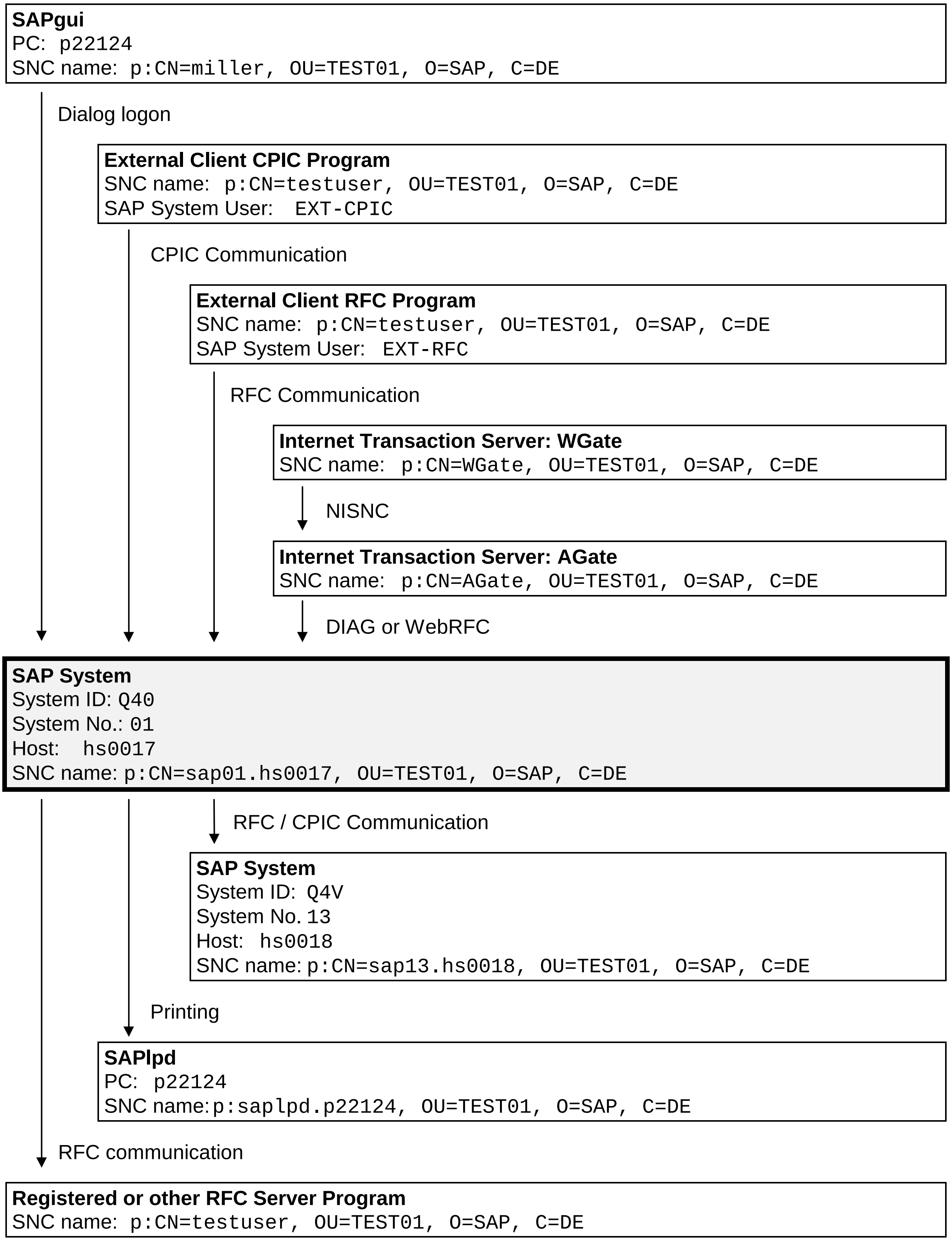
  You must link the programs using the current `rfclib`. The programs must access `saprfc.ini` and not `sideinfo` (which is normally the standard case anyway). Additionally, you need to update the configuration in the `saprfc.ini` file to include the SNC parameters.

- **Can I use SNC with R/2?**

  No.

Appendix A Sample SNC Scenario

The following are examples of SNC information for various components:



SAPgui
PC: `p22124`
SNC name: `p:CN=miller, OU=TEST01, O=SAP, C=DE`

Dialog logon

External Client CPIC Program
SNC name: `p:CN=testuser, OU=TEST01, O=SAP, C=DE`
SAP System User: `EXT-CPIC`

CPIC Communication

External Client RFC Program
SNC name: `p:CN=testuser, OU=TEST01, O=SAP, C=DE`
SAP System User: `EXT-RFC`

RFC Communication

Internet Transaction Server: WGate
SNC name: `p:CN=WGate, OU=TEST01, O=SAP, C=DE`

NISNC

Internet Transaction Server: AGate
SNC name: `p:CN=AGate, OU=TEST01, O=SAP, C=DE`

DIAG or WebRFC

SAP System
System ID: `Q40`
System No.: `01`
Host: `hs0017`
SNC name: `p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE`

RFC / CPIC Communication

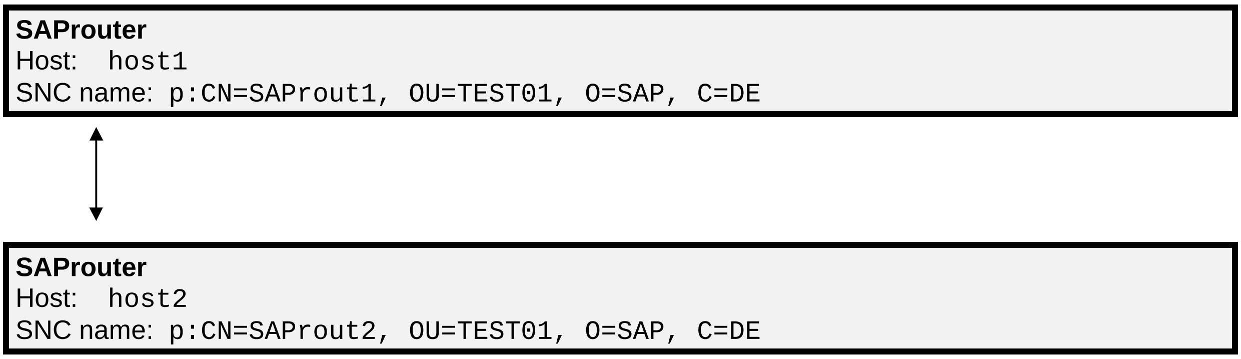
SAP System
System ID: `Q4V`
System No. 13
Host: `hs0018`
SNC name: `p:CN=sap13.hs0018, OU=TEST01, O=SAP, C=DE`

Printing

SAPlpd
PC: `p22124`
SNC name: `p:saplpd.p22124, OU=TEST01, O=SAP, C=DE`

RFC communication

Registered or other RFC Server Program
SNC name: `p:CN=testuser, OU=TEST01, O=SAP, C=DE`



SAProuter
Host: `host1`
SNC name: `p:CN=SAProut1, OU=TEST01, O=SAP, C=DE`

SAProuter
Host: `host2`
SNC name: `p:CN=SAProut2, OU=TEST01, O=SAP, C=DE`

Appendix B SNC-Related Tables

The following tables list the different tables in the SAP Systems that containSNC-relevant information.

Table A-1: SNC Tables Used for Incoming Connections

Table	Meaning
USRACL	This table contains the SNC name assignments for SAP System users. The SAP System verifies the entries in this table for all SNC logon requests from external clients (for example, SAPgui or external CPIC and RFC programs).
USRACLEXT	This table contains further SNC name assignments for SAP System users. It is used primarily for non-dialog users (RFC and CPIC). The SAP System verifies the entries in this table for SNC logon requests that use RFC or CPIC.
SNCSYSACL	This table contains the SNC names of the SAP Systems from which RFC and CPIC connections are to be accepted.

Table A-2: SNC Tables Used for Outgoing Connections

Table	Meaning
RFCDES	This table contains the RFC configuration, to include an indicator whether or not the connection should use SNC protection.
RFCDESSECU	This table contains additional SNC information for the RFC destination.
TXCOM	This table contains the CPIC configuration, to include an indicator whether or not the connection should use SNC protection.
TXCOMSECU	This table contains further SNC information for the CPIC destination.

Appendix C Maintenance Utilities

The standard SNC maintenance reports available in SAP Systems are shown in Table A-3.

Table A-3: SNC-Relevant RFC Functions

Report	Description
RSSNCCHK	Update a canonical SNC name
RSSNC40A	Convert SNC names from USR15 for Release 3.1 to USRACL for Release 4.0
RSUSR300	Set SNC names for all users (created over a template derived from the SAP System user)
RSUSR402	Create a file containing user information to be used by the external security product

Appendix D Special Cases Relevant to Releases 3.1G/H and 4.0A

D.1 Quality of Protection

The QoP for incoming and outgoing connections on the application server is handled differently in the Releases 3.1G/H and 4.0A than in later releases. The following explains the differences in more detail:

Profile parameter `snc/data_protection/max`

In these releases, the profile parameter `snc/data_protection/max` specifies the maximum protection level to apply to data being transferred. If data protected with a higher level than the value contained in the parameter is received, then an error occurs (SNCERR_OVERSECURE) and the transfer is terminated.

For outgoing connections, the value specifies the maximum level of protection to apply to the data. If a higher value is encountered, for example, in an RFC destination's profile, then the connection is terminated with an error.

QoP parameters: Permitted values

The minimum value allowed for the data protection parameters `snc/data_protection/min`, `snc/data_protection/max` and `snc/data_protection/use` is the value "2" (integrity protection). If you assign a value of "1" (authentication only) to any of these parameters, the value is automatically increased to "2".

Exception: A value of "1" is accepted if the security product does not support any higher levels of security.

Appendix E SNC Messages

SNC Start Messages

The SNC layer records SNC activation in the corresponding work process log files (`dev_w.`). It logs the relevant SNC information, to include:

- The QoP parameters and their values
- The path and file name of the external library
- The user or component's own SNC name

As of Release 4.5A, a message (RIQ) is also written to the system log.

Sample Work Process Log File Containing SNC Activation Messages

```
N  SncInit():   found snc/data_protection/max=3, using 3 (Privacy Level)
N  SncInit():   found snc/data_protection/min=3, using 3 (Privacy Level)
N  SncInit():   found snc/data_protection/use=3, using 3 (Privacy Level)
N  SncInit(): found snc/gssapi_lib=/usr/local/secude/lib/libsecude.sl
N    File " found snc/gssapi_lib=/usr/local/secude/lib/libsecude.sl "
        dynamically loaded as GSS-API V2 library.
N    The internal Adapter for the loaded GSS-API mechanism identifies as:
N    Internal SNC-Adapter (Rev 1.0) to SECUDE 5/GSS-API V2
N  SncInit(): found snc/identity/as=p:CN=sap01.hs0017, OU=TEST01, O=SAP,
        C=DE
N  SncInit(): Accepting  Credentials available, lifetime=Indefinite
N  SncInit(): Initiating Credentials available, lifetime=Indefinite
M  ***LOG R1Q=> p:CN=sap01.hs0017, OU=TEST01, O=SAP, C=DE & [thxxsnc.
        0228]
M  SNC (Secure Network Communication) enabled
```

SNC Trace Messages for the ITS

The SNC trace messages for the ITS are written to the files `WGate.trc`, `AGate.trc`, and `Mmanager.trc` on the corresponding hosts. A sample trace file after successful SNC installation is shown below:

Sample Trace File for the ITS

```
Fri Aug 08 13:36:17 1997
SncInit(): Trying environment variable SNC_LIB as a
gssapi library name: "c:\program files\secude\secude.dll"
File "c:\program files\secude\secude.dll" dynamically loaded as GSS-API
v2 library.
The internal Adapter for the loaded GSS-API mechanism identifies as:
Internal SNC-Adapter (Rev 1.0) to SECUDE 5/GSS-API v2
```

Appendix F Using SNC with MAC™OS

In this appendix, we describe the points that you need to take into consideration when configuringSNC under MAC™OS.

F.1 SAPgui

You cannot freely define the name of the external library (`SNC_LIB`) when using SAPgui with MAC™OS. The name of the library must be `GSSLibrary` and it must be located either in the same folder as the SAPgui executable file or in the *System Folder* under *Extensions*.

Configure the SNC options in MAC™OS SAP Logon, which is similar to SAP Logon under Windows.

For more information, see the SAP Logon `README` file. You can find it in the MAC™OS installation directory *SAPgui* → *Documentation*.

F.2 RFC Client Programs

As with other platforms, you configure SNC protection for RFC client programs under MAC™OS in the `saprfc.ini` file.

Although you can define the name of the external library in the parameter `SNC_LIB` as you wish, we recommend, as with SAPgui, that you use the name `GSSLibrary`.

In addition, as with SAPgui, the library must be located either in the same folder as the RFC client program or in the *System Folder* under *Extensions*.

RFC server programs from RFC SDK for MAC™OS are **not** supported. Likewise, CPIC client and server programs for MAC™OS are not supported.

Appendix G References

Ref.No.	Name and Location
[1]	**SAP Complementary Software (CSP™) Program** • http://www.sap.com/csp • http://www.sap.com/csp/scenarios/bc/bcsnc.htm
[2]	***SAP @ Web Installation Guide*** Material number: 51006024 or see the SAPNet link below and then choose the appropriate release: • http://sapnet.sap.com/instguides → *<Release>*
[3]	***R/3 Installation on Windows NT*** See the SAPNet link below and then choose the appropriate release: • http://sapnet.sap.com/instguides → *<Release>*
[4]	***X.509 Certificate Logon via the ITS*** See the SAPNet link below: • http://sapnet.sap.com/systemmanagement → *Security* → *Secure Network Communications*
[5]	**SAP library (R/3 library): *Internet Transaction Server*** • Release 4.0B: *CA – Cross-Application Components* → *Business Framework Architecture* → *Web Basis* → *R/3 Internet Application Components* → *R/3 Internet Application Components* → *Internet Transaction Server* (The path in other releases may vary.)
[6]	**SAP library (R/3 library): *BC – Printing Guide* (Transporting Printers and Device Types)** • Release 4.0B: *BC – Basis Components* → *Computing Center Management System* → *BC Printing Guide* → *BC Printing Guide* → *Defining and Modifying Device Types* → *Transporting a Device Type* and *Transporting Printers (Device Definitions)* (The path in other releases may vary.)
[7]	**SAP library (R/3 library): *BC SAProuter*** • Release 4.0B: *BC – Basis Components* → *Kernel Components* → *BC SAProuter* (The path in other releases may vary.)
[8]	**SAP library (R/3 library): *BC SAP Communication: CPI-C Programmer's Guide*** • Release 4.0B: *BC – Basis Components* → *Basis Services / Communication Interfaces* → *BC SAP Communication: CPI-C Programmer's Guide* (The path in other releases may vary.)
[9]	**SAPNet Note 66687: Use of network security products**
[10]	**SAPNet Note 150699: Latest patches for SNC-related problems**
[11]	**SAPNet Note 165485: R/3 server security under Windows NT**

Index

- /snc (SAPgui command line parameters) 4-2
- ~clientCert 4-45
- ~sncNameAGate 4-45
- ~sncNameR3 4-45
- ~sncQoPR3 4-45
- acceptor
  - application server 4-6, 4-8, 4-11, 4-16, 4-29
  - CPIC external program 4-31, 4-32
  - RFC external program 4-19, 4-20, 4-22, 4-23
  - SAPlpd 4-36
- access control lists (ACL)
  - systems 3-16, 3-19, 4-16, 4-17, 4-29, 4-46
  - users 3-16, 3-19, 3-22, 3-23, 3-25, 4-46
- AGate 4-44
- AGate.trc 4-45
- authentication 1-2
- authorization objects for RFC
  - S_RFC 3-16
  - S_RFCACL 3-16
- BACK (RFC destination) 4-25
- canonical names 2-3, 3-18, 3-22, 4-51, 4-52, A-4
- communication paths
  - overview 2-8
- CPIC
  - application server parameters 3-8
  - functions
    - SAP_CMACLKEY 4-51
    - SAP_CMACLKEYTONAME 4-51
    - SAP_CMNAMETOACLKEY 4-51
    - SAP_CMSNCMNAME 4-51
    - SAP_CMSNCMODE 4-51
  - maintaining destinations
    - in Customizing 3-17
    - tables used A-3
    - using SM54 .... 4-26, 4-31, 4-32
  - maintaining SNC options
    - for application servers 4-29
    - for external programs 4-10, 4-31, 4-32
    - general 4-26
  - transporting destinations 3-20
- cpictlib 4-10, 5-1
- C-program interfaces
  - CPIC 4-51
  - RFC 4-52
- credentials
  - belonging to application servers 4-16, 4-29
  - belonging to RFC external programs 4-20, 4-23, 4-24
  - belonging to the AGate 4-45
  - belonging to the WGate 4-44
  - definition 2-1
- Customizing 3-15, 3-18
- enable (SAPlpd parameters) 4-36
- external library
  - defined in SNC options
    - AGate 4-44
    - CPIC destinations 4-26
    - CPIC external programs 4-10, 4-31, 4-32
    - general 2-10, 2-11, 3-1
    - RFC destinations 4-12
    - RFC external programs 4-8, 4-19, 4-20, 4-22, 4-23
    - SAPgui 4-2
    - SAPlpd 4-36
    - WGate 4-43
  - definition 2-1
  - referenced by profile parameters
    - application server 3-4
    - gateway 3-13
- external names 2-1, 2-2, 2-6, 3-1, 3-21, 3-23
- external RFC server programs
  - defining SNC options
    - RFC destinations 4-12
    - start program on an application server 4-19
    - start program on an explicit host 4-20
  - gateway ports used 2-12
- external security products 1-1, 2-5, 2-6, 3-1, 3-17
- Frequently Asked Questions (FAQs) 5-1
- gateway operations
  - CPIC external programs 4-31, 4-32
  - ports 2-12, 4-9, 4-11

profile parameters 3-13
RFC external programs 4-21, 4-24
global.srvc 4-45
gssapi library
See ....external library
GSS-API V2....................2-1, 2-4, 2-5, 2-6, 3-4, 4-47, 4-48
gssapi_lib 4-36
gssapi32.dll 4-47, 4-48, 4-49
GSSLibrary A-6
gw/rem_start 3-14
GWSERV 4-11
identity/lpd 4-36
initiator
application server
for CPIC programs....................4-31, 4-32
for CPICs between SAP Systems....................4-29
for printing with SAPlpd 4-33
for RFC programs....................4-19, 4-20, 4-22, 4-23
for RFCs between SAP Systems....................4-15
external CPIC program....................4-10
external RFC program 4-7
SAPgui 4-1
SAProuter 4-39
integrity....................1-2
Internet Engineering Task Force (IETF)....................2-1, 2-4
Internet Transaction Server (ITS)....................4-43
LD_LIBRARY_PATH....................3-4
LIBPATH....................3-4
load balancing 4-15
logon screen....................3-26, 4-6
MAC™OS....................A-6
message server....................4-50
Mmanager.trc 4-45
NONE (RFC destination)....................4-25
NT LAN Manager Security Support Provider....................
(NTLMSSP)....................2-2, 4-47, 4-48
parameters
AGate
~clientCert 4-45
~sncNameAGate....................4-45
~sncNameR3....................4-45
~sncQoPR3....................4-45
SncNameAGate....................4-44
SncNameWGate....................4-44
Type....................4-44
application server
snc/accept_insecure_cpic ....
....................3-2, 3-9, 4-11, 4-30, 4-48
snc/accept_insecure_gui ....
.... 2-12, 3-2, 3-10, 3-21, 3-22, 4-6, 4-48, 4-49
snc/accept_insecure_r3int_rfc 3-2, 3-10, 4-18
snc/accept_insecure_rfc....................3-2, 3-11, 4-8, 4-17
snc/data_protection/max....................
....................3-2, 3-5, 4-14, 4-28, 4-45, 4-48, A-4
snc/data_protection/min.... 3-2, 3-6, 4-14, 4-48, A-4
snc/data_protection/use....................
....................3-2, 3-7, 4-14, 4-28, 4-48, A-4
snc/enable....................3-2, 3-3, 3-4, 3-21, 4-33, 4-48
snc/force_login_screen....3-2, 3-12, 3-21, 3-26, 4-6
snc/gssapi_lib ....
....................3-2, 3-4, 4-19, 4-20, 4-31, 4-32, 4-48
snc/identity/as 3-2, 3-5, 4-48
snc/permit_insecure_comm 3-2, 3-8
snc/permit_insecure_gui....................3-2, 3-9
snc/permit_insecure_start 3-2, 3-11
snc/r3int_rfc_qop 3-2, 3-8, 4-18
snc/r3int_rfc_secure....................
....................2-12, 3-2, 3-7, 4-18, 4-24, 4-25
snc/user_maint 3-2, 3-4
CPIC external programs
SNC_LIB....................4-10
SNC_MODE....................4-10
SNC_MYNAME....................4-10
SNC_PARTNERNAME....................4-10
SNC_QOP 4-10
gateway
GWSERV....................4-11
rem_start 3-14
snc/enable....................3-13, 4-21, 4-31
snc/gssapi_lib 3-13, 4-21, 4-31, 4-32
snc/permit_insecure_comm 3-13
snc/permit_insecure_start 3-13, 4-21, 4-31
RFC external programs
SNC_LIB....................4-8, 4-23
SNC_MODE....................4-8, 4-23
SNC_MYNAME....................4-8, 4-23, 4-24

SNC_PARTNERNAME 4-8
SNC_QOP..4-8, 4-23
SAPgui
/snc...4-2
SNC_LIB...4-2
SNC_MODE..4-2
SNC_PARTNERNAME 4-2
SNC_QOP...4-2
SAPlpd
enable 4-36
gssapi_lib 4-36
identity/lpd..4-36
WGate
SncNameAGate..4-44
SncNameWGate 4-44
Type 4-44
patents..2-4
ports...2-12, 2-13, 4-9, 4-11
printing.. 3-17, 3-20, 4-33
privacy 1-2
protection levels...1-2, 2-3, 2-10
See also .... Quality of Protection
QoP
See .... Quality of Protection
Quality of Protection
application server profile parameters 3-5, 3-6, 3-8
defined in SNC options
AGate..4-45
CPIC destinations 4-26, 4-28
CPIC external programs................ 4-10, 4-31, 4-32
RFC destinations 4-12, 4-14
RFC external programs.. ....4-8, 4-19, 4-20, 4-22, 4-23
SAPgui..4-2
SAPlpd..4-34, 4-37
SAProuter..4-41
with Microsoft NTLMSSP..................................4-49
definition...2-3
general 2-11
in Releases 3.1G/H and 4.0A A-4
See also ....protection levels
R/2 .... 4-15, 4-29, 5-1
recommendations...2-12
regulations 2-4
remote logons 4-24, 4-25
remsh, rsh..3-14, 4-21, 4-31
reports
RSSNC40A 3-16, A-4
RSSNCCHK...3-18, A-4
RSUSR300 ....2-7, 3-16, A-4
RSUSR402 ....3-17, A-4
RFC
application server parameters 3-7, 3-8, 3-10, 3-11
functions
RfcOpenEx...4-52
RfcSncAclKeyToName....................................4-52
RfcSncNameToAclKey....................................4-52
RfcSncPartnerAclKey 4-52
RfcSncPartnerName..4-52
maintaining destinations
in Customizing 3-17
tables used..A-3
using SM59................. 4-12, 4-13, 4-20, 4-22, 4-23
maintaining SNC options
for application servers 4-17
for external programs.... 4-7, 4-19, 4-20, 4-22, 4-23
for internal destinations 4-18
for logical destinations......................................4-19
for RFC groups 4-25
for SAPgui started per RFC..............................4-50
for special destinations......................................4-25
general..4-12
protecting internal destinations 2-12, 4-24, 4-25
transporting destinations 3-20
RFCDES...4-25, A-3
RFCDESSECU................................3-17, 4-12, 4-29, A-3
rfclib 4-7, 4-23, 5-1
RfcOpenEx..4-52
RfcSncAclKeyToName 4-52
RfcSncNameToAclKey 4-52
RfcSncPartnerAclKey...4-52
RfcSncPartnerName 4-52
route permission table 2-13, 4-39, 4-40, 4-41
RSSNC40A...3-16, A-4

- RSSNCCHK 3-18, A-4
- RSUSR300 2-7, 3-16, A-4
- RSUSR402 3-17, A-4
- SAP Complementary Software Program (CSP™) 2-6
- SAP Logon 4-1, 4-3, 4-49
- SAP Session Manager 4-1, 4-5
- SAP Shortcuts 4-1, 4-5
- SAP_CMACLKEY 4-51
- SAP_CMACLKEYTONAME 4-51
- SAP_CMNAMETOACLKEY 4-51
- SAP_CMSNCMODE 4-51
- SAP_CMSNCNAME 4-51
- sapdb<nn> 2-12
- SAPgui 3-9, 4-1, 4-22, 4-50
- sapgw<nn>s 2-12, 2-13, 3-13, 4-11
- SAPlpd 3-17, 3-20, 4-33, 4-36, 4-38
- saprfc.ini 4-7, 4-8, 4-23, 4-24, 4-52, 5-1, A-6
- SAProuter 2-12, 2-13, 4-39, 4-41
- service files 4-45
- SHLIB_PATH 3-4
- sideinfo 4-10, 4-11, 4-51, 5-1
- SIMG_BCSNC 3-15
- Single Sign-On 1-1, 2-2, 2-4, 4-47
- smart cards 1-1, 2-4
- SNC layer 2-4, 2-5
- SNC mode
  - CPIC destinations 4-26
  - CPIC external programs 4-10, 4-31, 4-32
  - CPIC functions 4-51
  - general 2-11
  - RFC destinations 4-12
  - RFC external programs 4-8, 4-19, 4-20, 4-22, 4-23
  - RFC functions 4-52
  - SAPgui 4-2
  - SAPlpd 4-36
- SNC names
  - AGate 3-23, 4-43, 4-44, 4-45, 4-46
  - application server
    - profile parameter 3-5
    - when communicating with AGate 4-45
    - when communicating with external programs
      - CPIC 4-10
      - RFC 4-8
    - when communicating with SAPgui 4-2
    - when maintaining CPIC destinations 4-26
    - when maintaining RFC destinations 4-12, 4-15
  - CPIC external programs 4-10, 4-31, 4-32
  - CPIC functions 4-51
  - definition 2-2
  - ITS Manager 4-44
  - message server 4-15
  - non-dialog users 3-23, 3-24
  - own names 2-10, 2-11
  - partner names 2-10, 2-11, 4-12, 4-26, 4-38, 4-51, 4-52
  - report RSUSR300 2-7
  - RFC external programs 4-8, 4-9, 4-19, 4-20, 4-22, 4-23
  - RFC functions 4-52
  - SAPlpd 4-34, 4-36
  - systems A-3
  - users 3-4, 3-21, 4-49, A-3
  - WGate 4-43, 4-44
- SNC protection 2-3, 2-9
- snc/accept_insecure_cpic 3-2, 3-9, 4-11, 4-30, 4-48
- snc/accept_insecure_gui 2-12, 3-2, 3-10, 3-21, 3-22, 4-6, 4-48, 4-49
- snc/accept_insecure_r3int_rfc 3-2, 3-10, 4-18
- snc/accept_insecure_rfc 3-2, 3-11, 4-8, 4-17
- snc/data_protection/max 3-2, 3-5, 4-14, 4-28, 4-45, 4-48, A-4
- snc/data_protection/min 3-2, 3-6, 4-14, 4-48, A-4
- snc/data_protection/use 3-2, 3-7, 4-14, 4-28, 4-48, A-4
- snc/enable 3-2, 3-3, 3-4, 3-13, 3-21, 4-21, 4-31, 4-33, 4-48
- snc/force_login_screen 3-2, 3-12, 3-21, 3-26, 4-6
- snc/gssapi_lib 3-2, 3-4, 3-13, 4-19, 4-20, 4-21, 4-31, 4-32, 4-48
- snc/identity/as 3-2, 3-5, 4-48
- snc/permit_insecure_comm 3-2, 3-8, 3-13
- snc/permit_insecure_gui 3-2, 3-9
- snc/permit_insecure_start 3-2, 3-11, 3-13, 4-21, 4-31
- snc/r3int_rfc_qop 3-2, 3-8, 4-18
- snc/r3int_rfc_secure 2-12, 3-2, 3-7, 4-18, 4-24, 4-25
- snc/user_maint 3-2, 3-4
- SNC_LIB

defined in SNC options
AGate....................4-44
CPIC external programs.................4-10, 4-31, 4-32
general....................2-11
RFC external programs....................4-8, 4-19, 4-20, 4-22, 4-23
SAPgui....................4-2
SAProuter....................4-40
WGate....................4-43
with MAC™OS....................A-6
with Microsoft NTLMSSP....................4-49
definition....................2-1
SNC_MODE....................2-11, 4-2, 4-8, 4-10, 4-23
SNC_MYNAME....................2-11, 4-8, 4-10, 4-23, 4-24
SNC_PARTNERNAME....................2-11, 4-2, 4-8, 4-10, 4-49
SNC_QOP....................2-11, 4-2, 4-8, 4-10, 4-23, 4-49
SNCERR_OVERSECURE....................A-4
SncNameAGate....................4-44
SncNameWGate....................4-44
SNCSYSACL
AGate entries....................3-25, 4-46
application server entries....................3-25, 4-16, 4-17, 4-18, 4-29, 4-30
general....................A-3
in Customizing....................3-16
transporting....................3-19
start messages....................A-5
tables
RFCDES....................A-3
RFCDESSECU....................3-17, 4-12, 4-29, A-3
SNCSYSACL
AGate entries....................4-46
application server entries....................3-25, 4-16, 4-17, 4-18, 4-29, 4-30
general....................A-3
in Customizing....................3-16
transporting....................3-19
TXCOM....................4-27, 4-29, 4-32, A-3
TXCOMSECU....................3-17, 4-26, 4-29, A-3
USR15....................3-18, A-4
USRACL....................3-16, 3-19, 3-22, 4-8, 4-11, A-3, A-4
USRACLEXT
AGate entries....................3-23, 3-25, 4-46
general....................A-3
in Customizing....................3-16
transporting....................3-19
user entries....................3-23, 3-24, 3-25, 4-9
trace files....................A-5
transactions
RZ10....................3-2
S070....................3-15
SM30
RFCDESSECU....................3-17, 4-12
SNCSYSACL....................3-19
TXCOMSECU....................4-26
USRACL....................3-16, 3-19, 3-22
USRACLEXT....................3-16, 3-19, 3-23, 3-24, 3-25
SM51....................4-24
SM54....................3-17, 4-26, 4-27, 4-31, 4-32
SM59.....3-17, 4-12, 4-13, 4-19, 4-20, 4-22, 4-23, 4-25
SNC0....................3-16, 4-16, 4-17, 4-29
SPAD....................4-33
SU01....................3-4, 3-16, 3-21, 3-23, 4-49
SUIM....................3-16
TXCOM....................4-27, 4-29, 4-32, A-3
TXCOMSECU....................3-17, 4-26, 4-29, A-3
Type....................4-44
user authentication....................4-9, 4-11, 4-18, 4-30
user maintenance
dialog users....................3-21
in Customizing....................3-16
non-dialog users....................3-23
profile parameters....................3-4
with Microsoft NTLMSSP....................4-49
USR15....................3-18, A-4
USRACL....................3-16, 3-19, 3-22, 4-8, 4-11, A-3, A-4
USRACLEXT....................3-16, 3-19, 3-23, 3-24, 3-25, 4-9, 4-46, A-3
views
RFCDESSECU....................3-17
TXCOMSECU....................3-17
USRACL....................3-16, 3-19
USRACLEXT....................3-16, 3-19
VSNCSYSACL....................3-16, 3-19, 4-46
VSNCSYSACL....................3-16

WebRFC.................................3-23, 3-25, 4-46

WGate.................................4-43

WGate.trc.................................4-44

win.ini.................................4-36

X.509 certificates.................................4-45