

# SAP Collections Management 6.0



## Copyright

© Copyright 2004 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

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

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.






JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

## Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

## Typographic Conventions

Type Style	Description
<i>Example text</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.  Cross-references to other documentation.
<b>Example text</b>	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example text	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
<b>Example text</b>	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

---

SAP Collections Management 6.0.....	5
Introduction .....	5
Before You Start .....	6
Technical System Landscape .....	7
User Management and Authentication .....	8
User Management.....	8
Integration with Single Sign-On Environments.....	10
Authorizations .....	11
Network and Communication Security.....	14
Communication Channel Security.....	15
Network Security .....	15
Communication Destinations.....	16
Data Storage Security .....	18
Trace and Log Files .....	18



# SAP Collections Management 6.0



## Introduction



This guide does **not** replace the daily operations handbook that we recommend customers to create for their specific productive operations.

## Target Group

- Technology consultants
- System administrators

This document is **not** included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

## The Need for Security

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using distributed systems, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system must **not** result in loss of information or processing time. These security requirements also apply to *SAP Collections Management*. To assist you in securing *SAP Collections Management*, we provide this Security Guide.

## About this Document

The Security Guide provides an overview of the security-relevant information that applies to *SAP Collections Management*.

### Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**

This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.
- **Technical System Landscape**

This section provides an overview of the technical components and communication paths that are used by *SAP Collections Management*.
- **User Management and Authentication**

This section provides an overview of the following user management and authentication aspects:

  - Recommended tools for user management.
  - User types required for *SAP Collections Management*
  - Standard users delivered with SAP Collections Management

- Overview of integration options in Single Sign-On environments
- **Authorizations**  
This section provides an overview of the authorization concept that applies to *SAP Collections Management*.
- **Network and Communication Security**  
This section provides an overview of the communication paths used by *SAP Collections Management* and the security mechanisms that apply.
- **Data Storage Security**  
This section provides an overview of the security mechanisms that *SAP Collections Management* uses for data storage.
- **Trace and Log Files**  
This section provides an overview of the trace and log files that contain information relevant for security. You can use these files to reproduce activities in the case of a security violation, for example.



## Before You Start

### Fundamental Security Guides

SAP Collections Management is based on *SAP NetWeaver* and *mySAP ERP*. Therefore, the corresponding Security Guides also apply to *SAP Collections Management*. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

#### Fundamental Security Guides

Scenario, Application or Component Security Guide
<i>SAP NetWeaver Security Guide</i>
<i>Financial Basis Security Guide</i>
<i>SAP ERP Central Component Security Guide</i>

For a complete list of all of the Security Guides published by SAP, see SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide).

### Additional Information

For more information about special topics, see the sources listed in the table below.

#### Further Information

Content	SAP Service Marketplace
Security	<a href="http://service.sap.com/security">service.sap.com/security</a>
Security Guides	<a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a>
Related SAP Notes	<a href="http://service.sap.com/notes">service.sap.com/notes</a>
Platforms permitted	<a href="http://service.sap.com/platforms">service.sap.com/platforms</a>

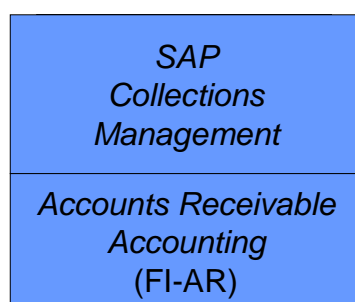
Network security	service.sap.com/network service.sap.com/securityguide
Technical infrastructure	service.sap.com/ti
<i>SAP Solution Manager</i>	service.sap.com/solutionmanager

## Technical System Landscape

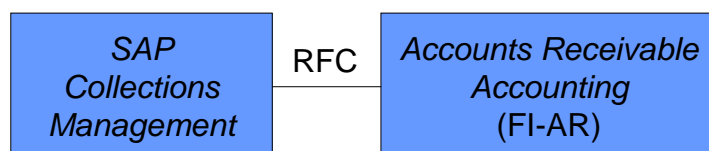
### Use

You can use *SAP Collections Management* as a **one-system** or as a **multiple-system scenario**. If you use *SAP Collections Management* in a one-system scenario, this means that you use Collections Management in the same system as Accounts Receivable. In a multiple-system scenario, you run Collections Management in a separate system. This communicates with the Accounts Receivable system connected by means of synchronous and asynchronous RFC calls and dialog calls.

The following figure shows an overview of the technical system landscape of *SAP Collections Management* in a one-system scenario.



The following figure shows an overview of the technical system landscape of *SAP Collections Management* in a multiple-system scenario.



For more information about the technical system landscape, see the sources listed in the table below.

### More Information About the Technical System Landscape

Subject	Guide/Tool	SAP Service Marketplace
Technical configuration High Availability	<i>Technical Infrastructure Guide</i>	service.sap.com/ti
Security		service.sap.com/security



## User Management and Authentication

For user management and authentication, *SAP Collections Management* uses the mechanisms of the *SAP NetWeaver* platform. Therefore, the corresponding security recommendations and guidelines of the user management and authentication for *SAP NetWeaver* also apply to *SAP Collections Management*.

In addition to these guidelines, we include information about user management and authentication that specifically applies to *SAP Collections Management* in the following topics:

- [User Management \[Seite 8\]](#)

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with *SAP Collections Management*.

- [Integration with Single-Sign-On Environments \[Seite 10\]](#)

This topic describes how *SAP Collections Management* supports Single Sign-On mechanisms.



## User Management

### Use

The user management of *SAP Collections Management* uses the mechanisms provided by *SAP NetWeaver* for the ABAP environment, for example, tools, user types, and password concept. For an overview of how these mechanisms affect *SAP Collections Management*, see the sections below. Furthermore, the system outputs a list of standard users that are required for operating *SAP Collections Management*.

### User Administration Tools

The following table shows the user management tools for *SAP Collections Management*.

#### User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance of <i>SAP NetWeaver</i> for the ABAP environment (transactions SU01 and PFCG)	For more information, see <a href="#">Users and Roles (BC-SEC-USR) [Extern]</a> .	



## User Types

It is often necessary to create different security policies for different types of users. For example, your policy may specify that users who perform their tasks interactively have to change their passwords on a regular basis, but not those users who perform their tasks using background processing.

Examples of user types required for *SAP Collections Management*:

- Individual users:
  - For each individual user in your system, you need dialog users for the following purposes:
    - To use the system via *SAP GUI for Windows*
    - If you use *SAP Collections Management* in a multiple system scenario and the RFC destinations used use a trusted-trusting system relationship, calls to the other system are performed using the current user from the calling system. Therefore, for each user a valid user must also exist in the target system.
- Technical users:
  - Background users can be used for processing in the background.
  - If you use *SAP Collections Management* in a multiple system scenario and the RFC destinations concerned are configured such that they do **not** use a trusted-trusting system relationship, you need the following technical users for the RFC destinations:
    - Communication users are used for synchronous and asynchronous BAPI calls (IDocs).
    - Dialog users are used for dialog calls that take place remotely in the other system.

For more information about these user types, see Security Guide for *SAP NetWeaver*.

## Standard Users

If you use *SAP Collections Management* in a multiple system scenario and there is **no** trusted-trusting system relationship between the systems involved, you have to configure corresponding users for the ALE/RFC communication between the systems involved.

Note that in *SAP Collections Management*, asynchronous BAPI calls (IDocs), synchronous BAPI calls, and dialog calls take place between the systems involved. There are calls from the Collections Management system to the system for Accounts Receivable Accounting and vice versa.

The following table shows the standard users required if you use *SAP Collections Management* in a multiple system scenario and there is **no** trusted-trusting system relationship between the systems involved.

**Standard Users**

System	User ID	Type	Password	Description
Collections Management system	Example: ALE-DIAG1	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Accounts Receivable Accounting system in the Collections Management system.
Collections Management system	Example: ALE-COMM1	Communication users	The user ID and password are stored in the RFC destination for the connection.	This user is used for synchronous BAPI calls or asynchronous BAPI calls (IDocs) from the Accounts Receivable Accounting system in the Collections Management system.
Accounts Receivable Accounting system	Example: ALE-DIAG2	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Collections Management system in the Accounts Receivable Accounting system.
Accounts Receivable Accounting system	Example: ALE-COMM2	Communication users	The user ID and password are stored in the RFC destination for the connection.	This user is used for synchronous BAPI calls or asynchronous BAPI calls (IDocs) from the Collections Management system in the Accounts Receivable Accounting system.

Create the users required and enter them in the corresponding RFC destinations. You can assign user IDs as required. The user IDs above are merely examples.



## Integration with Single Sign-On Environments

### Use

*SAP Collections Management* uses the Single Sign-On (SSO) mechanisms provided by *SAP NetWeaver*. Therefore, the security recommendations and guidelines for user management and authentication described in the *SAP NetWeaver Security Guide* also apply to *SAP Collections Management*.

The *Secure Network Communications* (SNC) mechanism is supported. SNC is available for user authentication and provides an SSO environment when the *SAP GUI for Windows* or *Remote Function Calls* (RFC) are used.

For more information, see the Security Guide for *SAP NetWeaver*.



## Authorizations

### Use

*SAP Collections Management* uses the authorization concept provided by *SAP NetWeaver*. Therefore, the corresponding security recommendations and guidelines for authorizations also apply to *SAP Collections Management*.

The *SAP NetWeaver* authorization concept is based on assigning authorizations to users based on roles. For role maintenance in *SAP NetWeaver* use the profile generator (transaction `PF03`).

### Standard Roles

The following table shows the standard roles delivered with *SAP Collections Management*.

#### Standard Roles

Role	Description
<b>SPECIALIST_COL_FSCM_FIN_SAP</b> <ul style="list-style-type: none"> <li>• One-system and multiple-system scenario</li> </ul>	<p><i>Collection Specialist</i></p> <p>Contains the authorizations that the collection specialist needs to perform the activities in his task area.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Calling the worklist</li> <li>• Displaying the business partner in <i>SAP Collections Management</i></li> <li>• Navigating to <i>Process Receivables</i></li> <li>• Creating contact persons in Collections Management</li> <li>• Creating promises to pay and dispute cases</li> <li>• Creating and changing customer contacts</li> <li>• Creating and changing resubmissions</li> </ul>

<p><b>MANAGER_COL_FSCM_FIN_AP</b></p> <ul style="list-style-type: none"> <li>• One-system and multiple-system scenario</li> </ul>	<p><i>Collection Manager</i></p> <p>Contains the authorizations that the collection manager needs to perform the activities in his task area.</p> <p>In addition to all authorizations of the <i>collection specialist</i> (role SAP_FIN_FSCM_COLL_SPECIALIST), this covers the following actions, for example:</p> <ul style="list-style-type: none"> <li>• Definition of collection strategies</li> <li>• Definition of collection groups</li> <li>• Assignment of a strategy to a group</li> <li>• Change the role of the business partner specific to <i>SAP Collections Management</i></li> <li>• Overview of several worklists</li> <li>• Distribution of worklist items to the collection specialists</li> </ul>
<p><b>ADMIN_COL_FSCM_FIN_SAP</b></p> <ul style="list-style-type: none"> <li>• One-system and multiple-system scenario</li> </ul>	<p><i>Collections Management Administrator</i></p> <p>Contains the authorizations that a user in the Collections Management system needs to start and monitor programs that run periodically and preferably in the background.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Worklist generation</li> <li>• Distribution of worklist items to the collection specialists</li> <li>• Mass change of the role of the business partner specific to <i>SAP Collections Management</i></li> <li>• Monitoring of parallel runs</li> <li>• Deletion of completed resubmissions</li> </ul>
<p><b>GDIALO_COL_FSCM_FIN_SAP</b></p> <ul style="list-style-type: none"> <li>• One-system scenario</li> </ul>	<p><i>Role for promise to pay functions</i></p> <p>Contains authorizations required by end users in Accounts Receivable so that they can call promise to pay functions in Accounts Receivable.</p> <p>Examples are:</p> <ul style="list-style-type: none"> <li>• Creating, displaying, and changing promises to pay from receivables processing in Accounts Receivable</li> <li>• Automatic change of promises to pay as a result of clearing transactions in Accounts Receivable</li> </ul>

<p><b>DIALOG_RFC_COL_FSCM_FIN_SAP</b></p> <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (dialog) for collections management functions</i></p> <p>Contains authorizations for a user with which dialog methods are called in the <i>SAP Collections Management</i> system from the Financial Accounting system by means of RFC.</p> <p>For example, navigation from receivables processing to the detail display of the promise to pay or dispute case.</p>
<p><b>COMM_RFC_COL_FSCM_FIN_SAP</b></p> <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (communication) for collections management</i></p> <p>Contains authorizations for a user with which synchronous and asynchronous methods are called in the <i>SAP Collections Management</i> system from the Financial Accounting system.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>Posting of IDocs with data from Financial Accounting</li> <li>Creation of dispute cases, promises to pay, customer contacts, and resubmission</li> <li>Reading of attributes of dispute cases, promises to pay, customer contacts, and resubmissions for display in receivables processing</li> </ul>
<p><b>USER_AR_COL_FSCM_FIN_SAP</b></p> <ul style="list-style-type: none"> <li>One-system and multiple-system scenario</li> </ul>	<p><i>End user in Receivables Processing</i></p> <p>Contains the authorizations required by an end user in receivables processing in Accounts Receivable.</p> <p>This role is in the Accounts Receivable system.</p>
<p><b>CO_RFC_AR_COL_FSCM_FIN_SAP MM</b></p> <ul style="list-style-type: none"> <li>Multiple-system scenario</li> </ul>	<p><i>RFC user (communication) in Accounts Receivable</i></p> <p>Contains authorizations for a user with which synchronous and asynchronous methods are called from the <i>SAP Collections Management</i> system in the Financial Accounting system.</p> <p>An example of such a method is the automatic notification to Accounts Receivable when promises to pay are confirmed and voided.</p>

<p><b>ADMIN_AR_COL_FSCM_FIN_SAP</b></p> <ul style="list-style-type: none"> <li>• One-system and multiple-system scenario</li> </ul>	<p><i>Collections Management Administrator Financial Accounting</i></p> <p>Contains the authorizations that a user in the Accounts Receivable system needs to start and monitor programs that run periodically and preferably in the background.</p> <p>For example, the transfer of data relevant for <i>SAP Collections Management</i> from Accounts Receivable:</p> <ul style="list-style-type: none"> <li>• Valuating Promises to pay</li> <li>• Automatic confirmation of promises to pay</li> </ul>
<p><b>DIA RFC_AR_COL_FSCM_FIN_SAP LOG</b></p> <ul style="list-style-type: none"> <li>• Multiple-system scenario</li> </ul>	<p><i>RFC user (dialog) in Receivables Processing</i></p> <p>Contains the authorizations for a user with which the navigate to receivables processing from the worklist by means of RFC. The authorizations permit the following activities:</p> <ul style="list-style-type: none"> <li>• Display of invoice data</li> <li>• Display of payment data</li> <li>• Display of invoice history</li> <li>• Creation, change, or display of a contact person</li> </ul>



## Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (*local area network*), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for *SAP Collections Management* is based on the topology used by the *SAP NetWeaver* platform. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to *SAP Collections Management*. Details that specifically apply to *SAP Collections Management* are described in the following topics:

- [Security of Communication Channels \[Seite 15\]](#)

This section describes the communication paths and logs used by *SAP Collections Management*.

-

[Network Security \[Seite 15\]](#)

This section describes the network topology recommended for *SAP Collections Management*. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate *SAP Collections Management*.

- [Communication Destinations \[Seite 16\]](#)

This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the *SAP NetWeaver Security Guide*:

- *Network and Communication Security*
- *Security Aspects for Connectivity and Interoperability*



## Communication Channel Security

### Use

The table below shows the communication paths used by *SAP Collections Management*, the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front end client using <i>SAP GUI for Windows</i> to application server	DIAG	All application data	Passwords
Application server to application server	RFC	Application data	

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

For more information, see *Transport Layer Security* in the *SAP NetWeaver Security Guide*.



## Network Security

Since *SAP Collections Management* is based on the technology of *SAP NetWeaver*, for information about network security, see the following sections of the *SAP NetWeaver Security Guide*:

- **Network Services**

This section contains information about services and ports that *SAP NetWeaver* uses.

- **Using Firewall Systems for Access Control**

This section contains information about firewall settings.

- **Using Multiple Network Zones**

This section contains information about which parts of your application should be set up in which network segments.



## Communication Destinations

### Use

The following table shows an overview of the communication destinations that you need for *SAP Collections Management* if you use it in a multiple-system scenario.

Destination	Delivered	Type	User, Authorizations	Description
Example: COL2FIN_DIAG	No	RFC	Under <a href="#">Authorizations [Seite 11]</a> , you can see the roles for dialog users that you need for dialog calls that take place from the Collections Management system to the Accounts Receivable system.	This destination is used for dialog calls that take place from the Collections Management system to the Accounts Receivable system by means of RFC.
Example: COL2FIN_COMM	No	RFC	Under <a href="#">Authorizations [Seite 11]</a> , you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Collections Management system to the Accounts Receivable system.	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Collections Management system to the Accounts Receivable system.
Example: FIN2COL_DIAG	No	RFC	Under <a href="#">Authorizations [Seite 11]</a> , you can see the roles for dialog users that you need for dialog calls that take place from the Accounts Receivable system to the Collections Management system.	This destination is used for dialog calls that take place from the Accounts Receivable system to the Collections Management system by means of RFC.
Example: FIN2COL_COMM	No	RFC	Under <a href="#">Authorizations [Seite 11]</a> , you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Accounts Receivable system to the Collections Management system.	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Accounts Receivable system to the Collections Management system.



You can assign names for your RFC destinations as required. The names of the RFC destinations used above are merely examples.

When you set up the RFC destinations for the ALE scenario, check whether the option of trusted/trusting system relationship is relevant for you. Using an RFC trusted/trusting system relationship between two SAP systems means that in the case of an RFC (Remote Function Call) from the trusted to the trusting system, **no** password is sent for the logon to the trusting system. You can configure the RFC destinations in such a way that the call in the target system occurs with the current user from the calling system without a password being specified or entered on the logon screen. This has the following advantages, for example:

- When changes to objects or data are logged in the called system, this logging takes place with the current user from the calling system. This makes it easier to track changes that occurred through RFC.
- You can assign individual authorizations to the users in the called system. As such you can differentiate which actions or functions are accessible to the user in the called system irrespective of the user.

With this procedure, you must create the users that are to be allowed to execute using RFC functions in the called system as well. Note that in the ALE scenario of *SAP Collections Management*, RFC calls take place from the Accounts Receivable system to the Collections Management system and vice versa. A trust relationship between SAP systems is **not** mutual. This means that you can choose whether one system is to be designated as trusted for the other system and vice versa, or whether you want to define the trust relationship only in one direction.

In the Customizing of ALE (Application Link Enabling), you can also define different RFC destinations for dialog calls, for BAPI calls, and for sending IDocs. As such you can also define an RFC destination for the dialog calls that use the trusted/trusting system relationship and use the current user from the calling system for the RFC calls in the target system, whilst you define an RFC destination for BAPI calls and for the sending of IDocs that does not use the trusted/trusting system relationship and in which you enter a communication user.



Note the following if your Accounts Receivable system is known as a trusted system by the Collections Management system and you want to configure the RFC destination used for sending IDocs so that it uses the trusted/trusting system relationship and carries out the RFC calls in the target system with the current user from the calling system:

IDocs are sent to the Collections Management system from the Accounts Receivable system when items are cleared in the Accounts Receivable system, the clearing of items is reset, or partial payments are executed on items for which a promise to pay exists for the corresponding invoice. If the corresponding RFC destination uses the trusted/trusting system relationship, and carries out the call in the target system with the current user from the calling system, this means that the user triggering the clearing, reset of clearing, or partial payment must also be defined in the Collections Management system. You must therefore create **all** users who carry out clearing, resets of clearing, or partial payments in the Accounts Receivable system, and therefore affect promises to pay, in the Collections Management system.



## Data Storage Security

### Use

Master data, transaction data, and Customizing data of *SAP Collections Management* is stored in the database of the SAP system.

Access to the database is restricted by the authorization objects of *SAP Collections Management*. To see the authorization objects relevant in *SAP Collections Management*, see the roles listed under [Authorizations \[Seite 11\]](#).



## Trace and Log Files

### Use

Changes to the business partner master data of *SAP Collections Management* are stored in the change documents of the business partner and in the history of the business partner specifically for *SAP Collections Management*.