

# SAP ECC Industry Extension Telecommunications Security Guide



Release 670

HELP.SECGUIDE\_TELCO



## 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 ECC Industry Extension Telecommunications Security Guide .....	5
Introduction .....	5
Before You Start.....	8
Technical System Landscape .....	9
Network and Communication Security.....	9



# SAP ECC Industry Extension Telecommunications Security Guide



## Introduction



This guide does not replace the daily operations handbook that SAP recommends customers create for their specific productive operations.

## Target Audience

- 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 a distributed system, 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 apply equally to *SAP ECC Industry Extension Telecommunications*. To assist you in securing *SAP ECC Industry Extension Telecommunications*, we provide this Security Guide.

## About this Document

The Security Guide provides an overview of the security-relevant information that applies to *SAP ECC Industry Extension Telecommunications*. This guide cross-references information in existing Security Guides where available, or other relevant documentation where security aspects are discussed.

Since *SAP ECC Industry Extension Telecommunications* contains *SAP Contract Accounts Receivable and Payable* (FI-CA or SAP RM-CA), you should also refer to the Security Guide for [Contract Accounts Receivable and Payable](#) if specific information for *SAP ECC Industry Extension Telecommunications* is not available in the following main sections:

### Overview of the Main Sections

The *SAP ECC Industry Extension Telecommunications* Security Guide comprises the following main sections:

- [Before You Start \[page 8\]](#)

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 \[page 9\]](#)

This section provides an overview of the technical components and communication paths that are used by *SAP ECC Industry Extension Telecommunications*.
- **User Administration and Authentication**

See the [User Administration and Authentication](#) section in the Contract Accounts Receivable and Payable Security Guide.

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

Recommended tools to use for user management:

  - User types required for Contract Accounts Receivable and Payable
  - Standard users supplied with Contract Accounts Receivable and Payable
  - Overview of the user synchronization strategy, if several components or products are integrated
  - Overview of integration options in single sign-on environments
- **Authorizations**

See the [Authorizations](#) section in the Contract Accounts Receivable and Payable Security Guide.

This section provides an overview of the authorization concept that applies to Contract Accounts Receivable and Payable.
- [Network and Communication Security \[page 9\]](#)

This section provides an overview of the communication paths used by SAP ECC Industry Extension Telecommunications and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

See the [Network and Communication Security](#) section in the Contract Accounts Receivable and Payable Security Guide.
- **Data Storage Security**

See the [Data Storage Security](#) section in the Contract Accounts Receivable and Payable Security Guide.

This section provides an overview of any critical data that is used by SAP ECC Industry Extension Telecommunications and the security mechanisms that apply.
- **More Security Information**

See the [More Security Information](#) section in the Contract Accounts Receivable and Payable Security Guide.
- **Trace and Log Files**

See the [Trace and Log Files](#) section in the Contract Accounts Receivable and Payable Security Guide.

This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

No specialist trace and log files are available for *SAP ECC Industry Extension Telecommunications*.



## Before You Start

### Security Guides Referenced

*SAP ECC Industry Extension Telecommunications* is based on *SAP NetWeaver* technology. This means that the Security Guide for *SAP NetWeaver* is also relevant.

Since *SAP ECC Industry Extension Telecommunications* contains *SAP Contract Accounts Receivable and Payable* (FI-CA or SAP RM-CA), you should also refer to the Security Guide for [Contract Accounts Receivable and Payable](#).

This means that the Security Guide for [ERP Central Component](#) is also relevant.

Both Security Guides are available in the *SAP Service Marketplace* at [service.sap.com/securityguide](http://service.sap.com/securityguide) → *mySAP ERP Security Guides*.

For a complete list of all available SAP security guides, see the SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide).

### Important SAP Notes

The most important SAP Notes that apply to *SAP ECC Industry Extension Telecommunications* security are shown in the table below.

SAP Note	Title	Remark
138498	Single Sign-On solutions	Contains information on single sign-on solutions.
853497	Adobe Acrobat Reader creates temporary files	References saving temporary files during use of the Adobe® Acrobat® Reader in SAP applications
783758	Security Guide ECC 5.0, 6.0	Provides any updates for the ERP Central Component guide and adds important information.

### Additional Information

For more information about specific topics, see the SAP Service Marketplace at [service.sap.com](http://service.sap.com) as shown in the table below.

Theme	Quick Link to SAP Service Marketplace
Security	<a href="http://service.sap.com/security">service.sap.com/security</a>
<i>SAP NetWeaver, ERP Central Component</i> Security Guide	<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	<a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a>
SAP Solution Manager	<a href="http://service.sap.com/solutionmanager">service.sap.com/solutionmanager</a>



## Technical System Landscape

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

Theme	Guide/Tool	Quick Link to the SAP Service Marketplace
Technical description of <i>SAP ECC Industry Extension Telecommunications</i> or the industry solution <i>SAP for Telecommunications</i> and the underlying technical components, such as <i>SAP NetWeaver</i>	Master Guide SAP for Telecommunications	<a href="http://service.sap.com/instguides">service.sap.com/instguides</a>
Security		<a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a>



## 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 risks relating to software flaws (at both the operating system and application level) or network attacks (such as sniffing). If users cannot log on to your application or database servers at the operating system or database level, then there is no way for malicious users (hackers) to compromise the machines and gain access to the database or files of the back-end system. 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 ECC Industry Extension Telecommunications* and Contract Accounts Receivable and Payable (FI-CA) is based on the topology used by *SAP NetWeaver*. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to *SAP ECC Industry Extension Telecommunications* and Contract Accounts Receivable and Payable (FI-CA). Details that relate directly to Contract Accounts Receivable and Payable (FI-CA) are described in the following sections:

- [Communication Channel Security](#)
- [Network Security](#)
- [Communication Destinations](#)



Please note the following security notes for communication with other systems for the following business scenarios and additional applications in *SAP ECC Industry Extension Telecommunications*:

- Business Scenario *Contract & Order Management* or management of telecommunications service locks in SAP CRM:

Communication between Contract Accounts Receivable and Payable (SAP-FI-CA) and SAP CRM uses the interfaces in the *SAP Exchange Infrastructure (XI)*. During configuration of the business scenario, a technical user must be set up in XI and Contract Accounts Receivable and Payable. XI uses these users for communication purposes.

- Invoicing in Contract Accounts Receivable and Payable

External billing systems supply billing documents for which invoice creation (posting in Contract Accounts Receivable and Payable and invoice printing) takes place during invoicing in Contract Accounts Receivable and Payable. Billing documents are imported using a BAPI interface (or ALE → IDoc). If billing documents from SAP CRM Billing are imported, communication takes place via the SAP CRM Middleware.