



SAP NetWeaver 2004s SPS 4  
Security Guide

# Security Guide ALE (ALE Applications)

Document Version 1.00 – October 24, 2005



SAP AG  
Neurottstraße 16  
69190 Walldorf  
Germany  
T +49/18 05/34 34 24  
F +49/18 05/34 34 20  
[www.sap.com](http://www.sap.com)

© Copyright 2005 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.

#### **Disclaimer**

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.






#### **Documentation in the SAP Service Marketplace**

You can find this documentation at the following Internet address:  
[service.sap.com/securityguide](http://service.sap.com/securityguide)

## 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.

## Icons

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*.

## Contents

Security Guide ALE (ALE Applications) .....	5
<b>1 General Security Measures (ALE) .....</b>	<b>5</b>
<b>2 Protecting the ALE Distribution Model .....</b>	<b>6</b>
<b>3 Measures to Take in the Source System .....</b>	<b>6</b>
<b>4 Measures to Take in the Target System .....</b>	<b>6</b>
4.1 Assigning Authorizations When Using Background Processing .....	7
4.2 Assigning Authorizations When Using Immediate Processing .....	7

# Security Guide ALE (ALE Applications)

Application Link Enabling (ALE) business processes are integrated processes across distributed systems.

ALE uses IDocs (intermediate documents) or BAPIs (Business Application Programming Interface) as data transfer format between the systems.

BAPIs are interfaces based on object-oriented technology. BAPIs can be called synchronously or asynchronously. Asynchronous BAPIs also use IDocs as data containers.

## Security Measures

Because ALE relies heavily on transactional RFC, all security issues that apply to RFC also apply automatically to ALE. You also need a well-established network infrastructure (see [Network Infrastructure \[SAP Library\]](#)).

The security measures specific to ALE apply to the ALE landscape configuration and the system user used for the communications. These measures are described in the following topics:

- [General Security Measures \(ALE\) \[Page 5\]](#)
- [Protecting the ALE Distribution Model \[Page 6\]](#)
- [Measures to Take in the Source System \[Page 6\]](#)
- [Measures to Take in the Target System \[Page 6\]](#)
- [Assigning Authorizations When Using Background Processing \[Page 7\]](#)
- [Assigning Authorizations When Using Immediate Processing \[Page 7\]](#)

## 1 General Security Measures (ALE)

Use the transaction SALE to maintain the ALE configuration, to include setting up the distribution model and setting up ALE user authorizations and profiles. Note the following:

- Be restrictive when assigning the ALE authorizations.  
The authorization profile B\_ALE\_ALL contains the following authorization objects that are needed for ALE:

### Authorizations for ALE

Authorization	Description
B_ALE_CGRP	ALE Customizing Distribution: Group Activities
B_ALE_LSYS	ALE/EDI: Maintaining logical systems
B_ALE_MAST	ALE/EDI: Distributing master data
B_ALE_MODL	ALE/EDI: Maintaining customer distribution model
B_ALE_RECV	ALE/EDI: Receiving IDocs via RFC
B_ALE_REDU	ALE/EDI: Generating messages (ex. reduction)
S_PROGRAM	ABAP: Program run checks
S_TABU_DIS	Table Maintenance (using standard tools such as SM30)

## 2 Protecting the ALE Distribution Model

- Protect external users and passwords.

For example, for a non-SAP system to send IDocs to a SAP System using transactional RFC, it must also send a SAP user ID and password. In most cases, the user and password are stored outside of the SAP System. Make sure that this information is not accessible to external systems or programs. (How you can do this is dependent on the system that you have; therefore, you need to refer to the documentation for the system where the information is stored.)

## 2 Protecting the ALE Distribution Model

Protect the ALE distribution model from unauthorized access by being restrictive with the maintenance authorization object B\_ALE\_MODL.

## 3 Measures to Take in the Source System

To make sure that users communicating over RFC in ALE are known to the sending system, you need to enter them and their logon information in the RFC destination. (Use transaction SM59). Therefore, set up these ALE users in the target system so that improper use is held to a minimum. (For more information, see [Measures to Take in the Target System \[Page 6\]](#).)

## 4 Measures to Take in the Target System

When defining the user for ALE in the target system, note the following:

- Set up special users for using ALE. Give only these users the authorizations for using ALE. Do not give the standard users authorizations for using ALE.
- The RFC users in the target system authorized to communicate in ALE with transactional RFC must be made known to the sender system. To prevent remote logons, assign the ALE users in the target system the type C (Communication) using transaction SU01. Do not assign them type *Dialog*, for the following reasons:
  - *Communication* users cannot execute dialog transactions.
  - *Dialog* users can remotely logon to an RFC destination from the maintenance transaction for RFC destinations (SM59).
- Restrict application authorization in the target system. You only need application authorizations in the target system if IDocs have to be processed immediately. IDocs should be processed as background jobs and not immediately, unless absolutely necessary.

See also:

- [Assigning Authorizations When Using Background Processing \[Page 7\]](#)
- [Assigning Authorizations When Using Immediate Processing \[Page 7\]](#)

## 4.1 Assigning Authorizations When Using Background Processing

If the IDocs transferred are to be processed using background processing (recommended), then note the following:

- In this scenario, the ALE users only require the authorization for creating and receiving IDocs. They do not need the authorization for the receiving application. You can therefore, restrict their authorizations to a minimum.
- The authorization object for receiving an IDoc is B\_ALE\_RECV. It contains the field EDI\_MES, which enables you to specify the message type that the user is authorized to receive.

## 4.2 Assigning Authorizations When Using Immediate Processing

If IDocs need to be processed immediately (instead of using background processing), then note the following:

- If inbound IDocs have to be transferred immediately to the application, the ALE user should only be assigned those application authorizations required to post the application document from the IDoc.
- Determine which authorizations are needed.