

# Discrete Industries and Mill Products (SAP ECC-DIMP) and SAP DBM: Security Guide



HELP.SECGUIDE\_DIMP

**Release 5.0**



## 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.

Discrete Industries and Mill Products (SAP ECC-DIMP) and SAP Dealer Business Management (SAP DBM): Security Guide .....	5
Introduction .....	5
Before You Start .....	6
Technical System Landscape .....	7
Technical System Landscape for SAP DBM .....	9
User Administration and Authentication.....	9
Authorizations .....	10
Authorizations for SAP DBM.....	12
Network and Communication Security.....	13
Communication Channel Security.....	14
Data Storage Security.....	17
Data Storage Security for SAP DBM .....	17
Other Security-Relevant Information .....	18



## Discrete Industries and Mill Products (SAP ECC-DIMP) and SAP Dealer Business Management (SAP DBM): Security Guide

In the following, you can find all the security information for the components SAP ECC DIMP and SAP Dealer Business Management (SAP DBM).

### Note on Security Guide Structure

As SAP DBM is an SAP ECC DIMP addon, all the security information for SAP ECC DIMP also applies to SAP DBM. You can find security information that only applies to SAP DBM in the relevant chapters. As SAP DBM is implemented in the automotive industry, pay particular attention to the information in this security guide regarding the automotive component and Vehicle Management System.



## Introduction



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

### Target Audience

This Security Guide is for the following target groups:

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Confirmation Guides, Technical Operations 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.

### Why Is Security Necessary?

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 on your system should not result in loss of information or processing time. These demands on security apply likewise to the SAP ECC DIMP component. To assist you in securing this component, we provide this Security Guide.

### About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP ECC DIMP.

### 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 the SAP ECC DIMP component.

- **User Administration and Authentication**

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

- **Authorizations**

This section provides an overview of the authorization concept that applies to the SAP ECC DIMP.

- **Network and Communication Security**

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

- **Data Storage Security**

This section provides an overview of any critical data that is used by SAP ECC DIMP and the security mechanisms that apply.



## Before You Start

### Fundamental Security Guides

The SAP ECC DIMP component is an addon for the SAP ERP Central Component (SAP ECC) and is built from the SAP NetWeaver technology. Therefore, the SAP ECC and SAP NetWeaver Security Guides also apply to SAP ECC DIMP. Pay particular attention to the security notes for authorizations in the SAP Web Application Server ABAP security guide.

#### Fundamental Security Guides

Security Guide	Available Under
SAP NetWeaver 04 Security Guide	SAP Service Marketplace under <b>service.sap.com/securityguide</b>
SAP ERP Central Component Security Guide	SAP Service Marketplace under <b>service.sap.com/securityguide</b>
SAP Web AS Security Guide – ABAP and Java	SAP Service Marketplace under <b>service.sap.com/securityguide</b>

For a complete list of the available SAP Security Guides, see SAP Service Marketplace at **service.sap.com/securityguide**.

### Important SAP Notes

The most important SAP Notes that apply to the security of SAP ECC-DIMP are shown in the table below.

#### Important SAP Notes

SAP Note Number	Description
727839	Role for SAP SCM - SAP ERP integration
829290	Role SAP_NFM_ALL for NF metals not available
794820	Collective note for enhancements to ECC DIMP security guide

## Additional Information

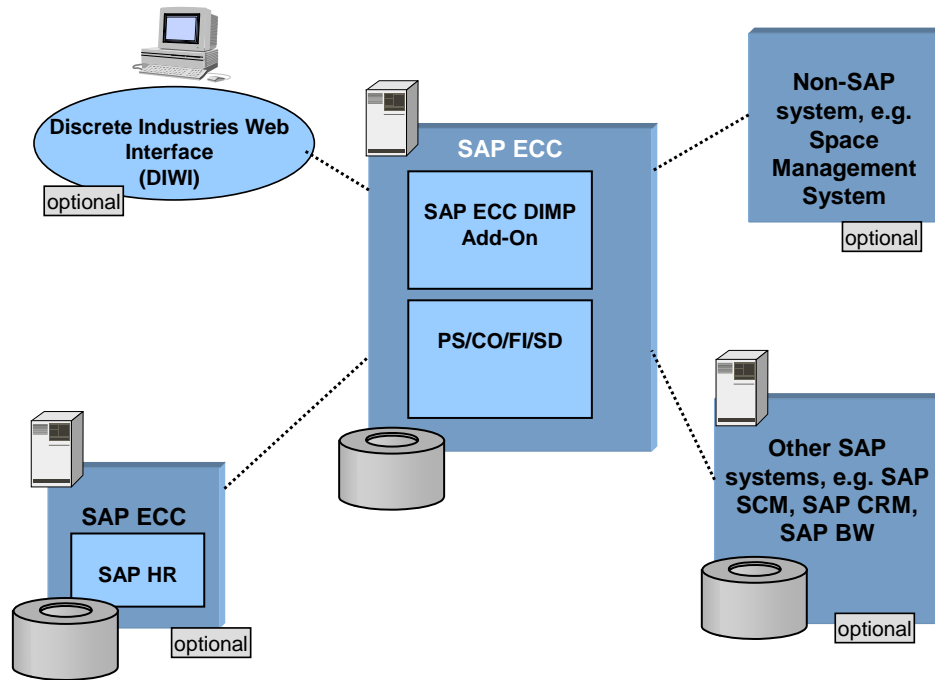
For more information about specific topics, see the Quick Links as shown in the table below.

### Quick Links to Additional Information

Content	Quick Link
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>
Released platforms	<a href="http://service.sap.com/platforms">service.sap.com/platforms</a>
Network security	<a href="http://service.sap.com/network">service.sap.com/network</a> <a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a>
<i>SAP Solution Manager</i>	<a href="http://service.sap.com/solutionmanager">service.sap.com/solutionmanager</a>

## Technical System Landscape

The figure below gives you an overview of the technical system landscape for the SAP ECC DIMP component.



At minimum, you need SAP ECC with the SAP ECC DIMP add-on. You need the *Discrete Industries Web Interface* for certain industries, for example, *Order to Delivery*. You can opt to implement non-SAP systems or another SAP ECC with SAP HR in accordance with your customer requirements. Depending on your business scenarios, you can also implement further SAP components, for example, SAP Supply Chain Management (SAP SCM) or SAP Customer Relationship Management (SAP CRM). For more information about the technical system landscape, see the resources listed in the table below:

**More Information About the Technical System Landscape**

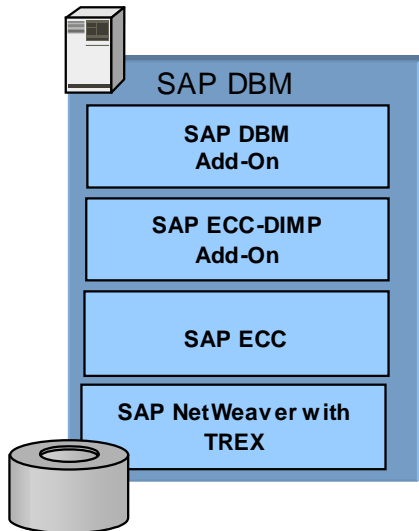
Content	Guide/Tool	Quick Link to the SAP Service Marketplace
Technical description for SAP ECC DIMP and the technical infrastructure of the industry solutions	Master Guide for Discrete Industries and Mill Products	<a href="http://service.sap.com/instguides">service.sap.com/instguides</a>
Technical description of the underlying technological component SAP NetWeaver	Master Guide for SAP NetWeaver	<a href="http://service.sap.com/instguides">service.sap.com/instguides</a>
Security		<a href="http://service.sap.com/security">service.sap.com/security</a>
Security of industry scenarios	Security Guide for industry scenarios	<a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a>
Configuration of industry scenarios	Configuration Guide or SAP Solution Manager	<a href="http://service.sap.com/ibc">service.sap.com/ibc</a> <a href="http://service.sap.com/solutionmanager">service.sap.com/solutionmanager</a>





## Technical System Landscape for SAP DBM

The following graphic gives you an overview of the technical system landscape for SAP DBM:



At minimum, you need to install SAP ECC with the SAP ECC DIMP and SAP DBM add-ons and TREX. Depending on your business scenarios, you may want to implement other components, for example, the components mentioned in the technical landscape for SAP ECC DIMP. If this is the case, check your installation and the available Master Guides at *SAP Service Marketplace* under **[service.sap.com/instguides](http://service.sap.com/instguides)**.

For more information about the technical system landscape for SAP ECC DIMP, see the [Technical System Landscape \[Page 7\]](#) section in this security guide.



## User Administration and Authentication

SAP ECC DIMP is an add-on for SAP ECC and is based on SAP NetWeaver and SAP Web Application Server (ABAP) technology. SAP ECC DIMP therefore uses SAP ECC and SAP NetWeaver user authorization and user authentication mechanisms. For more information, see the following security guides on *SAP Service Marketplace* at **[service.sap.com/securityguide](http://service.sap.com/securityguide)**:

- SAP NetWeaver 04 Security Guide
- SAP Web AS Security Guide for ABAP Technology
- SAP ECC Security Guide



## Authorizations

The SAP ECC DIMP component uses the authorization concept provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP also apply to SAP ECC DIMP.

The SAP Web Application Server authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the SAP Web AS ABAP.

As SAP ECC DIMP is an add-on for SAP ECC, you can use the roles and authorizations for SAP ECC. As well as the roles and authorizations delivered for SAP ECC, you can use the roles, profiles, and authorization objects described in the following for SAP ECC DIMP. Note that only the security-relevant roles and authorization objects are listed. For more information about roles and authorizations for SAP ECC, see the SAP ECC security guide under *Authorizations*.

## Standard Roles

### Mill Products

#### Non-Ferrous Metal Processing: Roles and Profiles

Role	Role Description	Profile
SAP_NFM_ALL	All authorizations in NF metals (/NFM/...) for the <i>Mill Products</i> industry solution	T_NFM_ALL0



If the role is not available in your system, see SAP Note 829290 to import the role.

## Standard Authorization Objects

### Aerospace & Defense

For Aerospace and Defense, you can use the authorization objects of the authorization class ISAD. For more information, see the documentation on authorization objects.

### Automotive

#### Standard Authorization Objects: Automotive

Area	Authorization Object	Description
Vehicle Management System (VMS)	C_AUTO_VMS	ISAUTO_VLC: Vehicle Management System
Cross-system transit between two plants	M_XLO_DEL	Assignment of goods issue to the delivery
Integrated Product and Process Engineering (iPPE)	C_PPE_PS	PS – iPPE Interface (Component Assignment)
	CPPE_PSI	PS – iPPE Interface (Interface)
	Authorization objects of the authorization object class PPE	
Production backflush	C_BCKFLUSH	Automotive: Production backflush

Warranty Processing	C_WTY_ACT	Warranty: action
	C_WTY_OBJ	Warranty: process object
	C_WTY_STAT	Warranty: status

For more information, see:

- Vehicle Management System

For more information, see the *SAP Help Portal* at [help.sap.com](http://help.sap.com) under *Documentation* → *SAP for Industries* → *SAP for Automotive* → *SAP ECC DIMP 5.0* → *Vehicle Management System* → *Vehicle Manager* → *Action* → *Execution of Actions*.

- Cross-system transit between two plants

You can find more information at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for Automotive* → *SAP ECC-DIMP 5.0* → *Cross-System Transit Between Two Plants*.

## Engineering, Constructions & Operations

You can use the following authorization objects for Engineering, Construction and Operations:

Area	Authorization Object	Description
Equipment and Tools Management (ETM)	J_3GBLART	Authorizations for document types
	J_3GEQART2	CEM – Equipment Types for Document Category 2
	J_3GEMPGR2	CEM - Recipient Groups, Document Category 2
	J_3GBEWTP2	CEM – Transaction Types, Document Category 2
	J_3GACTVT	CEM Allowed Activities
	J_3GABRLST	Call CEM Settlement List for Organizational Units
	J_3GDUMMY1	Dummy Maintenance
	J_3G_DUMMY	Dummy Maintenance
	J_3GTESTSD	Enhanced Test Environment for SD Order Input
	J_3GDISPGR	MRP Group in Equipment
	P	Planning Area in Recipient
	J_3G_TCODE	Transaction Code
Homebuilding	H_BROWSE	Community browser of the homebuilding solution
	H_AFFECTED	Maintenance of dependencies between buildings
	H_FITLIST	Maintenance Object for Product Fit List
	H_AUTOGEN	Mass Generation Tool of Homebuilding
	H_RULES	Rules Maintenance of the homebuilding solution

For more information, see the documentation on authorization objects.

## High Tech

For High Tech, you can use the authorization objects of the authorization class ISHT. The following authorization objects of authorization class SD is also available:

Authorization object	Description
V_SMPA_ACT	Authorization object for the component IS-HT-SW
V_SMPA_FUN	Authorization object for the component IS-HT-SW
V_SMPA_TCD	Authorization object for the component IS-HT-SW
V_SMPA_VAR	Authorization object for the component IS-HT-SW

For more information, see the documentation on authorization objects. You can find more information about the authorization objects for *Distributor Reseller Management (DRM)* at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for High Tech* → *SAP ECC DIMP 5.0* → *Manufacturer/Supplier Processes* → *Distributor Reseller Management* → *List of Authorization Objects*.

## Critical Combinations

There are no known critical combinations of authorizations.



## Authorizations for SAP DBM

The SAP DBM component uses the authorization concept provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP also apply to SAP DBM.

The SAP Web Application Server authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the SAP Web AS ABAP.

As SAP DBM is an add-on for SAP ECC-DIMP, you can use the roles and authorizations for SAP ECC. As well as the roles and authorizations delivered for SAP ECC and SAP ECC-DIMP, you can use the roles, profiles, and authorization objects described in the following for SAP DBM.

## Standard Roles

You can use the following roles specifically for SAP DBM:

Role	Description
/DBM/CDESK	General role for cash desk
/DBM/CUST	General role for customer
/DBM/ORDER	General role for order
/DBM/PACKAGE	General role for package
/DBM/VEHICLE	General role for vehicle

The roles use the authorization objects mentioned in the next section.

## Standard Authorization Objects

You can use the following authorization objects specifically for SAP DBM:

Authorization Object	Description
/DBM/CDESK	Cash desk
/DBM/CUST	Authorization object for customer
/DBM/ORDER	Authorization object for order
/DBM/PCKG	Authorization object for packages
/DBM/VEH	Authorization object for vehicle



## 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 ECC DIMP 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 ECC DIMP. Details that specifically apply to SAP ECC DIMP are described in [Communication Channel Security \[Page 14\]](#).

As SAP ECC DIMP is an add-on for SAP ECC, pay attention to the information about network and communication security for SAP ECC in the SAP ECC Security Guide under the following sections:

- **Communication Channel Security**  
This topic describes the communication paths and protocols used by SAP ECC.
- **Network security**  
This topic describes the recommended network topology for SAP ECC.
- **Communication Destinations**  
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

### General

In following, you will find an overview of the communication channels for SAP ECC DIMP with the following information:

- Communication paths that use the SAP ECC DIMP component
- The protocol for the connection
- Type of data transferred

The overview is limited to the communication paths that are specific to SAP ECC DIMP. For more information about communication paths that use SAP ECC, see the SAP ECC Security Guide on the SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide) → *SAP ECC Security Guide*.

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 the SAP NetWeaver Security Guide on the SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide) → *SAP NetWeaver 04 Security Guide (Complete)* → *SAP NetWeaver Security Guide* → *Network and Communication Security* → *Transport Layer Security*.

### Aerospace & Defense

#### Maintenance and Service Planning

##### Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP SCM System – SAP ECC DIMP System	RFC	Application data	-
SAP SCM System – SAP BW System	RFC	Application data	-

For more information on security for the *Maintenance and Service Planning* Business Scenario, see the Security Guide for SAP SCM 4.1 and the *Maintenance and Service Planning Security Guide* on the *SAP Service Marketplace* at [service.sap.com/securityguide](http://service.sap.com/securityguide).

### Automotive

#### Production Backflush (ISA-PPC)

##### Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP SCM System – SAP ECC DIMP System	RFC	Application data	-

For more information on the communication paths, see the documentation on production backflush in the SAP Help Portal at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for Automotive* → *SAP ECC DIMP 5.0* → *Production Backflush* → *Customizing Settings for the Production Backflush*.

For more information on communication path security, see the SAP SCM 4.1 Security Guide on the SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide).

## Vehicle Management System (VMS)

### Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP ECC DIMP System - IPC	HTTP	Application data	-
SAP ECC DIMP System – SCEM System	RFC	Application data	-
SAP ECC DIMP System – SAP BW System	RFC	Application data	-
SAP ECC DIMP System - TREX	RFC	Application data	-
SAP ECC DIMP System – SAP CRM System	RFC	Application data	-
SAP ECC DIMP System – DIWI System	HTTP	Application data	-
SAP ECC DIMP System – SAP Enterprise Portal System	HTTP	Application data	-

Note the following regarding system connections and data protection:

- For system connections between the SAP ECC DIMP System, SAP Customer Relationship Management (SAP CRM) and SAP Business Information Warehouse (SAP BW) you can use the technical user ALEREMOTE.



Read SAP Note 727839 if working with the ALEREMOTE user.

- The *Vehicle Management System* role concept contains a security policy for vehicles and end customers. If you use the *Dealer Portal* and want to control how data for users is displayed, implement this visibility concept. For more information, see the *Vehicle Management System* in the SAP Help Portal at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for Automotive* → *SAP ECC DIMP 5.0* → *Vehicle Management System (IS-A-VMS)* → *Master Data* → *Role*.
- For more information, see the *Vehicle Management System* in the SAP Help Portal at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for Automotive* → *SAP ECC DIMP 5.0* → *Vehicle Management System (IS-A-VMS)* → *Technical Integration*.
- For more information on communication channel security, see the Security Guide for the appropriate component: SAP NetWeaver, SAP CRM, SAP BW, SAP Enterprise Portal and SAP SCM on the SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide).

## Cross-system transit between two plants

### Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP ECC DIMP System – SAP ECC DIMP System	RFC	Application data (IDocs)	-

## Supplier Workplace

You can only use an SAP ECC DIMP system for the Supplier Workplace. Your supplier uses a web browser to access data. Alternatively, you can use an SAP Enterprise Portal. For more information about the system landscape for the Supplier Workplace, see the SAP Help Portal at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for Automotive* → *SAP ECC DIMP 5.0* → *Supplier Workplace*.

### Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP ECC DIMP System on customer side – Browser on supplier side	HTTP	Application data	All transferred data
SAP ECC DIMP System – SAP Enterprise Portal System on customer side	HTTP	Application data	All transferred data
SAP Enterprise Portal System – Browser on the supplier side	HTTP	Application data	All transferred data

## High Tech

### Distributor Reseller Management (IS-HT-DRM)

#### Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP ECC DIMP System – EDI Subsystem	ASCII or other protocol that supports data exchange with IDocs	Application Data (sales and distribution data and inventory data)	-

For more information, see the *Distributor Reseller Management* documentation in the *SAP Help Portal* at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for High Tech* → *SAP ECC DIMP 5.0* → *Distributor Reseller Management*.

## Mill Products

### Communication Paths



Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP ECC DIMP System – SAP SCM System	RFC	Application data	

You can use the technical user ALEREMOTE for system connections.



Read SAP Note 727839 if working with the ALEREMOTE user.

For more information on communication path security, see the SAP SCM 4.1 Security Guide on the SAP Service Marketplace at [service.sap.com/securityguide](http://service.sap.com/securityguide).



## Data Storage Security

### Aerospace & Defense

The system saves sensitive data in the logbook application. The system saves the data in various object types (log entry, log notification, log measurement document). You can use a combination of authorization checks and business add-ins (BAIs) to protect this data.

For each object type, the system checks whether you have authorizations for the following:

- Creating an object from the logbook
- Displaying an object from the logbook
- Changing an object from the logbook
- Removing an object from the logbook

When you select a structure node in the object navigation structure, the display authorization check defines whether you can display the details for an object. The change authorization check defines whether you can change to change mode on the detail screen.

These authorization checks do not cover all possible eventualities. Therefore, the logbook application also offers BAIs for checking authorizations. For more information, see the logbook application documentation in the SAP Help Portal at [help.sap.com](http://help.sap.com) → *Documentation* → *SAP for Industries* → *SAP for Aerospace & Defense* → *SAP ECC DIMP 5.0* → *Maintenance, Repair and Overhaul (MRO)* → *Maintenance and Service Processing* → *Logbook*, and the documentation for the AUTHORITY\_CHECK\_ACL business add-in.



## Data Storage Security for SAP DBM

In the cash desk functions, SAP DBM only stores the payment type (cash, EC, Visa, MC, check). Credit card numbers are not stored. When checking a customer's credit limit, the system accesses the open items and the customer's credit limit. This access is secured by the SAP authorization concept.

SAP DBM uses some HR data. This data is protected by the SAP authorization concept.



## Other Security-Relevant Information

In *Maintenance and Service Processing* you can also use digital signatures for the logbook. For more information about using digital signatures with the logbook, see the *SAP Help Portal* under **help.sap.com** → *Documentation* → *SAP for Industries* → *SAP for Aerospace & Defense* → *Maintenance and Service Processing* → *Logbook* → *Certification*. For more security-relevant information about digital signatures, see the documentation for SAP NetWeaver in the SAP Help Portal at **help.sap.com** → *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 04* → *Security* → *Digital Signatures and Encryption*.