SAP Auto-ID Infrastructure 2.1: Security Guide

ADDON.ERPSECGUIDE_RFID

Release 210

Copyright

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
Example text	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.
Example text	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.
`Example text`	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 Auto-ID Infrastructure 2.1: Security Guide

Introduction

This guide does not replace the daily operations handbook that we recommend 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, whereas 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 of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP Auto-ID Infrastructure. To assist you in securing SAP Auto-ID Infrastructure, we provide this Security Guide.

As SAP Auto-ID Infrastructure is based on other SAP products, we strongly recommend that you consult the SAP NetWeaver Security Guide and the SAP Supply Chain Management Security Guide as well.

About this Document

SAP Auto-ID Infrastructure is an out-of-the-box solution that integrates RFID technology with existing SAP logistics systems, and delivers a generic infrastructure that enables integration with heterogeneous system landscapes.

The solution comprises of one or more Auto-ID infrastructure systems, which can be implemented on various types of platforms ranging from PDAs and workstations to large servers.

SAP Auto-ID Infrastructure offers the following system integration options:

1. Integration between SAP Auto-ID Infrastructure and an SAP supply chain execution backend system.
2. Integration between SAP Auto-ID Infrastructure and SAP Supply Chain Event Management.
3. A combination of options 1and 2.
4. Integration between SAP Auto-ID Infrastructure and a third-party backend system. This will require respective configuration.

You can integrate SAP Auto-ID Infrastructure with any RFID device controllers or fixed RFID devices that support HTTP communication.

For information about the integration with SAP Auto-ID Infrastructure, see the SAP Help Portal **`http://help.sap.com`** under *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Auto-ID Infrastructure* → *Integration*.

This security guide provides security-relevant information for the component SAP Auto-ID Infrastructure (SAP AII 2.1).

This security guide also provides security-relevant information for the scenario *RFID-Enabled Outbound Processing* based on SAP Auto-ID Infrastructure 2.1.

For information about the scenario *RFID-Enabled Outbound Processing*, see *Business Scenario Configuration Guide: RFID-Enabled Outbound Processing* in the SAP Service Marketplace under **`service.sap.com/ibc`** → *mySAP SCM*.

As SAP Auto-ID Infrastructure can be integrated with other SAP and non-SAP products, you will sometimes find security-relevant information about other SAP and non-SAP products which will help to secure SAP Auto-ID Infrastructure.

Conversely, a lot of security-relevant information about other SAP and non-SAP products can only be found in the specific security guides of these products.

For information about fundamental security guides of SAP Auto-ID Infrastructure, see Before You Start [Page 6].

In many cases the required information has already been provided in other security guides and in configuration and installation guides. In these cases, the guide provides a reference to the relevant units.

All security guides are available at: **`http://service.sap.com/securityguide`**.

Before you start

Fundamental Security Guides

Fundamental Security Guides

Application	Guide	Most relevant sections or specific restrictions
SAP WebAS	SAP NetWeaver Security Guide	In the *SAP NetWeaver Security Guide*, choose *Security Guides for SAP NetWeaver Products* → *SAP Web Application Server Security Guide.*
SAP Exchange Infrastructure 3.0	SAP NetWeaver Security Guide	In the *SAP NetWeaver Security Guide*, choose *Security Guides for SAP NetWeaver Products* → *SAP Security Guide XI*.
SAP R/3 4.6C, SAP R/3 Enterprise 4.7 Extension Set 100 and 200	SAP WebAS Security Guide	
SAP SCM 4.1	SAP SCM 4.1 Component Security Guide	
Operating Systems and	SAP NetWeaver Security	In the *SAP NetWeaver*

Database Platforms	Guide	*Security Guide*, choose *Operating System and Database Platform Security Guides*.

For a complete list of the available SAP Security Guides, see the Quick Link **/securityguide** on the *SAP Service Marketplace*.

You can find all security guides and other security-relevant documentation for SAP Auto-ID Infrastructure as follows:

Guide/Documentation	**Full path to the guide**
SAP Auto-ID Infrastructure Installation Guide	SAP Note: 777426
SAP Auto-ID Infrastructure documentation	**help.sap.com** → *mySAP Business Suite* → *mySAP SCM* → *SAP Auto-ID Infrastructure*
RFID–Enabled Outbound Processing Configuration Guide	**service.sap.com/ibc** → *mySAP SCM* → *SAP RFID solution package* → *Business Scenario Configuration Guide* → *RFID-Enabled Outbound Processing: Configuration Guide*
SAP NetWeaver Security Guide	**service.sap.com/securityguide** or **help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver 04* To navigate to the security guide in the SAP NetWeaver documentation, choose *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide*.
SAP NetWeaver documentation	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver 04*
SAP WebAS Security Guide	**service.sap.com/securityguide**
SAP NetWeaver '04 Installation Guide	**service.sap.com/instguides** → *SAP NetWeaver* → *Release 04* → *Installation*
SAP NetWeaver '04 Installation Guide - SAP Exchange Infrastructure 3.0	**service.sap.com/instguides** → *SAP NetWeaver* → *Release 04* → *Installation*
SAP Exchange Infrastructure 3.0: Configuration Guide	**service.sap.com/instguides** → *SAP NetWeaver* → *Release 04* → *Installation*
SAP Supply Chain Management Documentation (SAP SCM Documentation)	**help.sap.com** → *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Supply Chain Management*
SAP Supply Chain Management Security Guide (SAP SCM Security Guide)	**service.sap.com/securityguide**

Important SAP Notes

The most important SAP Notes that apply to the security of SAP Auto-ID Infrastructure are shown in the table below.

Important SAP Notes

SAP Note Number	Title	Comment
723780	Security Guide: SAP Auto-ID Infrastructure	The note covers all problems discovered after the publication of the security guide, and provides additional information about security issues.
138498	Single Sign-On Solutions	Information on Single Sign-On solutions for SAP systems

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 on the SAP Service Marketplace
Security	**security**
Security Guides	**securityguide**
Related SAP Notes	**notes**
Released platforms	**platforms**
Network security	**network** **securityguide**
Technical infrastructure	**ti**
SAP Solution Manager	**solutionmanager**

Technical System Landscape

Use

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

More Information About the Technical System Landscape

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace
Technical description for SAP Auto-ID Infrastructure and the underlying technological components such as SAP NetWeaver	Master Guide	**service.sap.com/instguides**
Technical configuration High Availability	Technical Infrastructure Guide	**service.sap.com/ti**
Security		**service.sap.com/security**

User Administration and Authentication

SAP Auto-ID Infrastructure uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP Web AS Security Guide for ABAP Technology* also apply to SAP Auto-ID Infrastructure.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP Auto-ID Infrastructure in the following topics.

User Management

Use

User management for SAP Auto-ID Infrastructure uses the mechanisms provided by the SAP Web Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP Auto-ID Infrastructure, see the sections below. In addition, we provide a list of the standard users required for operating SAP Auto-ID Infrastructure.

User Administration Tools

The table below shows the tools to use for user management and user administration with SAP Auto-ID Infrastructure.

User Management Tools

Tool	Detailed Description
User Management Engine (UME) administration console	Use the web-based UME administration console to maintain users, roles and authorizations in Java-based systems that use the UME for the user store, for example, the SAP Web AS Java and the Enterprise Portal. The UME also supports various persistency options, such as ABAP Engine or a directory server.
SAP Web AS Java user management using the Visual Administrator	Use the Visual Administrator to maintain users and roles on the SAP Web AS Java. The SAP Web AS Java also supports a pluggable user store concept. The UME is the default user store.
User Management for the ABAP Engine (transaction code **SU01**)	Use the user management transaction SU01 to maintain users in ABAP-based systems.
Profile Generator (transaction code **PFCG**)	Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.
Central User Administration (CUA)	Use the CUA to centrally maintain users for multiple ABAP-based systems. Synchronization with a directory server is also supported.

For a detailed description of the user management tools available in SAP NetWeaver, see the SAP Service Marketplace **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *User Management* → *User Management Tools*.

User Types

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

For more information on these user types, see User Types in the *SAP Web AS ABAP Security Guide*.

Standard Users

The table below shows the standard users or user groups that are necessary for operating SAP Auto-ID Infrastructure. It also includes some SAP WebAS, SAP XI and SAP Event Management (SAP EM) users or user groups.

Standard Users

System	User ID	Type	Password	Description
SAP WebAS	<sapsid>adm	SAP System Administrator	To be entered	*SAP NetWeaver '04 Installation Guide*
SAP WebAS	SAPService <sapsid>	SAP System Service Administrator	To be entered	*SAP NetWeaver '04 Installation Guide*
SAP WebAS	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	See SAP NetWeaver Security Guide	See SAP NetWeaver Security Guide	*SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver Products* → *SAP Web Application Server Security Guide* → *SAP Web AS Security Guide for ABAP Technology* → *User Authentication* → *Protection Standard Users*
SAP WebAS	SAP Standard SAP Web AS Java Users (Administrator, Guest, Emergency)	See SAP NetWeaver Security Guide	See SAP NetWeaver Security Guide	*SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver Products* → *SAP Web Application Server Security Guide* → *SAP Web AS Security*

				Guide for Java Technology → Users and User Management → Standard Users and Groups
SAP Auto-ID Infrastructure	SAP AII User	Dialog user	To be entered	*SAP Auto-ID Configuration Guide → User Administration → Users and roles in SAP AII*
SAP Auto-ID Infrastructure	SAP AII WebDynpro Communication User	Communication user	To be entered	*SAP Auto-ID Installation Guide → Installing SAP AII 2.1 → Maintaining JCo Connections → Using Name/Password for Connection to Backend*
SAP XI  This information is only relevant if you have already installed this component	SAP XI User	Communication user	To be entered	*SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → General Activities*
SAP EM  This information is only relevant if you have already installed this component	SAP Event Management Users	Dialog user	To be entered	SAP SCM Documentation → *SAP Event Management (SAP EM) → Supply Chain Coordination → Uses of Supply Chain Event Management → SAP Event Management User*
SAP ECC or SAP R/3	SAP backend Users	Dialog user	To be entered	*Business Scenario Configuration Guide: RFID-Enabled Outbound Processing → User Administration → User Maintenance in SAP R/3 and*

				SAP XI

For information about SAP NetWeaver standard users, see the SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *SAP Web AS Security Guide for ABAP Technology* → *User Authentication* → *Protecting Standard Users*.

For information about SAP NetWeaver password rules, see the SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver* → *Release 04* → *Security* → *Identity Management* → *Users and Roles (BC-SEC-USR)* → *User Maintenance* → *Logon and Password Security in the SAP System* → *Password Rules*.

User Data Synchronization

Use

To avoid administrational effort, the use of user data synchronization could be useful in your system landscape. As the component SAP Auto-ID Infrastructure is based on SAP NetWeaver, all the mechanisms for user data synchronization of SAP NetWeaver are available for SAP Auto-ID Infrastructure.

For information about user data synchronization, see the SAP Service Marketplace at **`http://service.sap.com/securityguide`** under *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *Integration of User Management in Your System Landscape*.

Integration into Single Sign-On Environments

Use

SAP Auto-ID Infrastructure supports the Single Sign-On (SSO) mechanisms provided by the SAP Web Application Server Java and ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP Web Application Server Security Guide* also apply to SAP Auto-ID Infrastructure.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides for an SSO environment when using SAP GUI for Windows or Remote Function Calls.

For more information, see *Secure Network Communications (SNC)* in the *SAP Web Application Server Security Guide*.

SAP logon tickets

SAP Auto-ID Infrastructure supports the use of logon tickets for SSO when using a Web browser as the front end client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.

You can find more information under *SAP Logon Tickets* in the *SAP Web Application Server Security Guide*.

Client certificates

As an alternative to user authentication using a user ID and passwords, users using a Web browser as a front end client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

You can find more information under *Client Certificates* in the *SAP Web Application Server Security Guide*.

Authorizations

Use

SAP Auto-ID Infrastructure uses the authorization 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 Auto-ID Infrastructure.

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 SAP Web AS ABAP.

Standard Roles

The table below shows the standard roles that are used by SAP Auto-ID Infrastructure.

Standard Roles

System	Role	Description
SAP AII	SAP_AIN_ADMINISTRATOR (The roles SAP_XI_APPL_SERV_USER and SAP_XI_MONITOR_ABAP are also needed for the AII administrator)	*RFID–Enabled Outbound Processing Configuration Guide* → *User Administration* → *Users and Roles in SAP AII* **and** SAP Auto-ID Infrastructure system documentation (transaction code **PFCG**)
SAP AII	SAP_XI_MONITOR_ABAP	*RFID–Enabled Outbound Processing Configuration Guide* → *User Administration* → *Users and Roles in SAP AII* **and** SAP Auto-ID Infrastructure system documentation (transaction code **PFCG**)
SAP AII	SAP_AIN_SUPERVISOR	*RFID–Enabled Outbound Processing Configuration Guide* →

		User Administration → Users and Roles in SAP AII **and** SAP Auto-ID Infrastructure system documentation (transaction code **PFCG**)
SAP AII	SAP_AIN_WORKER	*RFID–Enabled Outbound Processing Configuration Guide → User Administration → Users and Roles in SAP AII* **and** SAP Auto-ID Infrastructure system documentation (transaction code **PFCG**)
SAP ECC or SAP R/3	SAP_LE_AID_IDOC_ADMIN	Auto-ID backend IDoc administration
SAP ECC or SAP R/3	SAP_LE_AID_DATA_DISPLAY	Auto-ID backend data display
SAP ECC or SAP R/3	SAP_QM_CA_OUTCERT_MAINT	Administration of Certificate Master Data
SAP ECC or SAP R/3	SAP_MM_PUR_MESSAGE_MAINTENANCE	General Message Maintenance in Purchasing
SAP ECC or SAP R/3	SAP_LO_HU_MASTER_DATA	Master Data for Handling Units
SAP ECC or SAP R/3	SAP_CFM_ADMINISTRATOR	Administrator
SAP ECC or SAP R/3	SAP_AUDITOR	AIS - Audit Information System

For information about roles for SAP WebAS, SAP XI and SAP EM, see the *SAP NetWeaver Security Guide* and the *SAP SCM Security Guide* at the SAP Service Marketplace at **`http://service.sap.com/securityguide`**.

Authorizations for the WebDynpro Connection Users

The users that are used for the WebDynpro connection need an authorization role or an authorization profile containing the following authorization objects:

WebDynpro Connection	Authorization Object
AII_WD_MODELDATA_DEST	/AIN/UI_RFC
AII_WD_RFC_METADATA_DEST	S_RFC

For information about the required authorization objects for the WebDynpro connections, see the *SAP Auto-ID Infrastructure Installation Guide → Installing AII 2.1 → Maintaining JCo Connections → Using Name/Password for Connection to Backend.*

Authorizations for Configuration in SAP ECC or SAP R/3

For the configuration of the SAP ECC or SAP R/3 backend system within the *RFID-Enabled Outbound Processing* business scenario use the possibility to create IMG customizing roles.

For information about how to create roles, see the SAP Help Portal at **`http://help.sap.com`** under *SAP NetWeaver → Release 04 → Security → Identity Management → Users and Roles (BC-SEC-USR) → SAP Authorization Concept → Organizing Authorization Administration → Organization if You Are Using the Profile Generator → Role Maintenance.*

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 Auto-ID Infrastructure 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 Auto-ID Infrastructure. Details that specifically apply to SAP Auto-ID Infrastructure are described in the following topics.

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

As communication channels transfer all kinds of your business data, they should be protected against unauthorized access. SAP offers general recommendations and technologies to protect your system landscape based on SAP NetWeaver.

You should activate the Secure Network Communication (SNC) for RFC and Secure Sockets Layer Protocol (SSL) for http within all communication channels in SAP Auto-ID Infrastructure to achieve a secure system landscape.

For information about the communication security of SAP NetWeaver, see the SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

For information about security aspects for connectivity and interoperability of SAP NetWeaver, see the SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Security Aspects for Connectivity and Interoperability*.

As SAP Auto-ID Infrastructure can be used with mobile devices like mobile RFID devices, a special focus on the communication channel security is necessary. As the mobile devices are connected via http, the Secure Sockets Layer Protocol (SSL) should be used for securing the communication.

We strongly advise that you only use mobile devices which can communicate via Secure Sockets Layer Protocol (SSL).

For information about mobile devices within SAP Auto-ID Infrastructure, see the SAP Help Portal at **`http://help.sap.com`** → *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Auto-ID Infrastructure* → *Getting Started* → *Other Auto-ID Concepts* → *RFID Device*.

The table below shows the communication paths used by Auto-ID Infrastructure, the protocol used for the connection and the type of data transferred.

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front end client using SAP GUI for Windows to application server	DIAG	All application data	e.g. Passwords, business data
Front end client using a Web browser to application server	HTTP(S)	All application data	e.g. Passwords, business data
Application server to application server	RFC, HTTP(S)	Integration data	Business data
Application server to third-party application	HTTP(S)	All application data	e.g. Passwords, Business data

For more information about communication paths and the data sent and received within SAP Auto-ID Infrastructure, see the SAP Help Portal at **`http://help.sap.com`** → *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Auto-ID Infrastructure* → *Integration* → *Integration With SAP Systems*.

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.

If you use SAP Exchange Infrastructure for the integration of SAP Auto-ID Infrastructure, consult also the SAP XI Security Guide.

Network Security

Use

Your network infrastructure is extremely important in protecting your system. 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.

SAP offers general recommendations to protect your system landscape based on SAP NetWeaver.

For information about network security of SAP NetWeaver, see the SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

A minimum security demand for your network infrastructure is the use of a firewall for all your services provided via the Internet.

A more secure variant is to protect your systems (or groups of systems) by locating the different "groups" in different network segments, each protected with a firewall against unauthorized access. (Note: external security attacks can also come from "inside" if the intruder has already taken over control of one of your systems.)

For information about access control using firewalls, see the SAP Service Marketplace at **`http://service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security - Using Firewall Systems for Access Control*.

Communications Destinations

Use

Users and authorizations for connection destinations can cause high security flaws in instances of careless use

Golden Rules for connection users and authorizations:

- Choose user type “communication” or "system".
- Assign only the minimum required authorizations to the user.
- Choose a secure and secret password for the user.
- Store only connection user logon data for users of type “connection” or "system".
- Choose "trusted system" functionality when ever possible instead of storing connection user logon data.

The table below shows an overview of the communication destinations used by SAP Auto-ID Infrastructure. To give a better overview the communication destinations for SAP XI, SAP SCM and SAP ECC / SAP R/3 are also listed.

Connection Destinations

Destination	JCo WebDynpro Connection: AII_WD_MODELDATA_DEST
Delivered	Preconfigured
Type	JCo Connection
User, Authorizations	Authorization Object: /AIN/UI_RFC
Description	SAP Auto-ID Infrastructure Installation Guide → Installing AII 2.1 → *Maintaining JCo Connections*

Destination	JCo WebDynpro Connection: AII_WD_RFC_METADATA_DEST
Delivered	Preconfigured
Type	JCo Connection
User, Authorizations	Authorization Object: S_RFC
Description	SAP Auto-ID Infrastructure Installation Guide → *Installing AII 2.1* → *Maintaining JCo Connections*

Destination	SAP AII → SAP XI
Delivered	No
Type	RFC - HTML
User, Authorizations	User role: SAP_XI_APPL_SERV_USER

Description	SAP Auto-ID Infrastructure Documentation → *Integration → Integration With SAP Systems → Integration With SAP Supply Chain Execution Landscape → SAP Auto-ID Infrastructure – SAP Backend System Communication* **and** SAP Auto-ID Infrastructure Documentation → *Integration → Integration With SAP Systems → Integration with mySAP SCM → SAP Auto-ID Infrastructure – SAP EM Backend System Communication* **and** *RFID-Enabled Outbound Processing Configuration Guide → Auto-ID Infrastructure Configuration → Setting up an RFC Destination from SAP AII to SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server*

Destination	SAP AII → SAP XI <SAPSLDAPI>
Delivered	No
Type	RFC - TCP/IP
User, Authorizations	-

Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server → Creating a Connection Between a Business System and the System Landscape Directory (SLD)*

Destination	SAP AII → SAP XI <LCRSAPRFC>
Delivered	No
Type	RFC – TCP/IP
User, Authorizations	-
Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server*

Destination	SAP AII → RFIDdevices / device controller
Delivered	No
Type	HTTP
User, Authorizations	-

Description	SAP Auto-ID Infrastructure Documentation → *Integration → Integration With SAP Systems → Integration with RFID Devices* **and** *RFID-Enabled Outbound Processing Configuration Guide → Auto-ID Infrastructure Configuration → Maintaining Device Settings* **and** SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with SAP Supply Chain Execution Landscape → SAP Exchange Infrastructure (SAP XI) Configuration* **and** SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with mySAP SCM → SAP Exchange Infrastructure (SAP XI) Configuration* **and** *RFID-Enabled Outbound Processing Configuration Guide → Auto-ID Infrastructure Configuration → Setting up an RFC Destination from SAP AII to SAP XI* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Configuration of a Central Integration Server → Defining HTTP Destinations for Business Systems*

Destination	SAP XI → SAP AII
Delivered	No
Type	RFC - HTTP
User, Authorizations	-

Description	SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with SAP Supply Chain Execution Landscape → SAP Exchange Infrastructure (SAP XI) Configuration* **and** SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with mySAP SCM → SAP Exchange Infrastructure (SAP XI) Configuration* **and** *RFID-Enabled Outbound Processing Configuration Guide → Auto-ID Infrastructure Configuration → Setting up an RFC Destination from SAP AII to SAP XI* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Configuration of a Central Integration Server → Defining HTTP Destinations for Business Systems*

Destination	SAP XI → SAP XI <LCRSAPRFC>
Delivered	No
Type	RFC – TCP/IP
User, Authorizations	-
Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Activities for SAP Exchange Infrastructure → Creating RFC Destinations in the ABAP and Java Environments*

Destination	SAP XI → SAP XI <SAPSLDAPI>
Delivered	No
Type	RFC – TCP/IP
User, Authorizations	-

Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Activities for SAP Exchange Infrastructure → Creating RFC Destinations in the ABAP and Java Environments*

Destination	SAP XI → SAP SCM (SAP EM)
Delivered	No
Type	RFC- R/3
User, Authorizations	See references
Description	SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with mySAP SCM → SAP Exchange Infrastructure (SAP XI) Configuration* **and** *RFID–Enabled Outbound Processing Configuration Guide → Integration with SAP SCM (SAP Event Management) → Settings in SAP XI for Integration with SAP SCM → Defining an RFC Connection to SAP SCM (Event Management)* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server*

Destination	SAP XI → SAP ECC or SAP R/3
Delivered	No
Type	RFC- R/3
User, Authorizations	See references

Description	SAP Auto-ID Infrastructure Documentation ® *Integration → Integration with SAP Systems → Integration with SAP Supply Chain Execution Landscape → SAP Exchange Infrastructure (SAP XI) Configuration* **and** *RFID–Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Setting up RFC Destinations from the SAP XI to SAP R/3* **and** *SAP Exchange Infrastructure (XI) 3.0 Configuration Guide → Integration of Business Systems Using the IDoc Adapter → Settings of the Integration Server System*

Destination	SAP SCM (SAP EM) → SAP XI
Delivered	No
Type	RFC – R/3
User, Authorizations	User role: SAP_XI_APPL_SERV_USER
Description	SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with mySAP SCM → SAP Exchange Infrastructure (SAP XI) Configuration* **and** *RFID-Enabled Outbound Processing Configuration Guide → Integration with SAP SCM (SAP Event Management) → Settings in SAP SCM for Integration with SAP R/3 and SAP XI → Defining Target Systems for RFC Destinations in SAP SCM* **and** *SAP Exchange Infrastructure (XI) 3.0 Configuration Guide → Preparation → Service Users and Assigned Roles* **and** *SAP Exchange Infrastructure (XI) 3.0 Configuration Guide → Integration of Business Systems Using the IDoc Adapter → Settings for the IDoc Sending System (R/3)*

Destination	SAP SCM (SAP EM) → SAP XI <SAPSLDAPI>
Delivered	No
Type	RFC - TCP/IP
User, Authorizations	-

Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server → Creating a Connection Between a Business System and the System Landscape Directory (SLD)*

Destination	SAP SCM (SAP EM) → SAP XI <LCRSAPRFC>
Delivered	No
Type	RFC – TCP/IP
User, Authorizations	-
Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server*

Destination	SAP SCM (SAP EM) → SAP ECC or SAP R/3
Delivered	No
Type	RFC – R/3

User, Authorizations	Use the Profile Generator (transaction **PFCG**) to define an appropriate profile
Description	*RFID-Enabled Outbound Processing Configuration Guide → Integration with SAP SCM (SAP Event Management) → Settings in SAP SCM for Integration with SAP R/3 and SAP XI → Defining Target Systems for RFC Destinations in SAP SCM* **and** SAP SCM Documentation → *SAP Event Management (SAP EM) → System Installation and Integration*

Destination	SAP ECC or SAP R/3 → SAP XI
Delivered	No
Type	RFC – R/3
User, Authorizations	User role: SAP_XI_APPL_SERV_USER
Description	SAP Auto-ID Infrastructure Documentation → *Integration → Integration with SAP Systems → Integration with SAP Supply Chain Execution Landscape → SAP Exchange Infrastructure (SAP XI) Configuration* **and** *RFID-Enabled Outbound Processing Configuration Guide → Definition of IDocs from SAP R/3 to SAP XI → Defining Target Systems for RFC Calls* **and** *SAP Exchange Infrastructure (XI) 3.0 Configuration Guide → Preparation → Service Users and Assigned Roles* **and** *SAP Exchange Infrastructure (XI) 3.0 Configuration Guide → Integration of Business Systems Using the IDoc Adapter → Settings for the IDoc Sending System (R/3)*

Destination	SAP ECC or SAP R/3 → SAP XI <SAPSLDAPI>
Delivered	No
Type	RFC - TCP/IP
User, Authorizations	-

Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server → Creating a Connection Between a Business System and the System Landscape Directory (SLD)*

Destination	SAP ECC or SAP R/3 → SAP XI <LCRSAPRFC>
Delivered	No
Type	RFC – TCP/IP
User, Authorizations	-
Description	*RFID-Enabled Outbound Processing Configuration Guide → Configure the Service Landscape in SAP XI → Maintaining the System Landscape Directory (SLD) in SAP XI* **and** *SAP NetWeaver Installation Guide - SAP Exchange Infrastructure 3.0 → Post-Installation Activities → Creating RFC Destinations in the ABAP Environment* **and** *Creating RFC Destinations in the ABAP and Java Environments* **and** *SAP Exchange Infrastructure (XI) 3.0: Configuration Guide → Connecting Business Systems with an Integration Engine to the Central Integration Server*

Destination	SAP ECC or SAP R/3 → SAP SCM (SAP EM)
Delivered	No
Type	RFC - R/3

User, Authorizations	Use the Profile Generator (transaction **PFCG**) to define an appropriate profile
Description	*RFID-Enabled Outbound Processing Configuration Guide → Integration with SAP SCM (SAP Event Management) → Settings in SAP R/3 for Integration with SAP SCM → Defining Target Systems for RFC Calls* **and** SAP SCM Documentation → *SAP Event Management (SAP EM) → System Installation and Integration*

 SAP EM and SAP XI connections are only relevant if you implement SAP EM and SAP XI.

Data Storage Security

Use

The data storage security of SAP NetWeaver and components installed on this base is described in detail in the SAP NetWeaver Security Guide.

For information about the data storage security of SAP NetWeaver, see the SAP Service Marketplace at **http://service.sap.com/securityguide** → *SAP NetWeaver Security Guide → Operation System and Database Platform Security Guides*.

Security for Additional Applications

Use

You can integrate SAP Auto-ID Infrastructure with any RFID device controllers or fixed RFID devices that support HTTP communication. As this RFID device controllers or fixed RFID devices are non-SAP products, we suggest you consult the documentation of the RFID products used regarding security.

The RFID device controller or fixed RFID devices should be able to communicate via the Secure Sockets Layer Protocol (SSL) to ensure a secure communication.

For more information about RFID device controllers or fixed RFID devices, see Communication Channel Security [Page 15] and the SAP Help Portal at **http://help.sap.com** under *mySAP Business Suite → mySAP Supply Chain Management ® SAP Auto-ID Infrastructure → Getting Started → Other Auto-ID Concepts → RFID Device*.

To date, there are no RFID device controllers or fixed RFID devices that support an authentication mechanism (only an identification mechanism). Due to this fact, you should be aware that masquerading or spoofing is possible in an insecure environment.

Dispensable Functions with Impacts on Security

Test Client

The SAP Auto-ID Infrastructure comes with the report *AIN HTTP Test Client* (transaction code **/AIN/HTTP_TEST**). This report is for testing HTTP requests and has no impact on the system security. As it is not necessary for the daily operation of SAP Auto-ID Infrastructure, the report is not included into the SAP Menu.

This report can be deactivated in your system by locking the transaction **/AIN/HTTP_TEST** using transaction **SM01**.

Other Security-Relevant Information

Web Browser as User Front End

To use the Web browser as user front end, it is necessary to activate Java script (Active Scripting) to ensure a working user interface.

This could conflict with your security policy regarding web services.

For more information about the web user interface for SAP Auto ID Infrastructure and SAP WebDynpro, see the SAP Service Marketplace at **service.sap.com/webdynpro,** or the SAP Library at **help.sap.com** under *SAP Web Application Server → SAP Web Application Server 6.30 → Choose English → SAP NetWeaver Components → SAP Web Application Server → J2EE Technology in SAP Web Application Server → Development Manual → Developing Web Applications → Web Dynpro.*

Trace and Log Files

All trace and log files of SAP Auto-ID Infrastructure use SAP NetWeaver standard mechanisms.

For information about the trace and log files of SAP NetWeaver, see the SAP Service Marketplace at **http://service.sap.com/securityguide** → *SAP NetWeaver Security Guide*.