SAP Auto-ID Infrastructure 5.1: Security Guide

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 5.1: 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 1 and 2.
4. Integration between SAP Auto-ID Infrastructure and a third-party backend system. This will require respective configuration.
5. Integration in an Object Event Repository (OER)

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 SAP Help Portal at **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 5.1).

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 **service.sap.com/securityguide**.

Before You Start

Fundamental Security Guides

Application	Guide	Most relevant sections or specific restrictions
SAP NetWeaver 2004s	SAP NetWeaver Security Guide	*SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guides for the Usage Type AS* **and**: → *Security Guides for the Usage Type PI* **and**: → *Security Guides for the Usage Type BI*
SAP ECC 6.0	SAP ERP Central Component Security Guide	
Operating Systems and Database Platforms	SAP NetWeaver Security Guide	*SAP NetWeaver Security Guide* → *Security Guides for DB and OS 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 Note	SAP Note: 1022171
SAP Auto-ID Infrastructure documentation	**help.sap.com** → *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Auto-ID Infrastructure*
RFID-Enabled Outbound and Inbound Processing: Configuration Guide	**service.sap.com/rfid** → Detailed Information
SAP NetWeaver Security Guide	**service.sap.com/securityguide** or: **help.sap.com** → *Documentation* → *SAP NetWeaver* To navigate to the security guide in the SAP NetWeaver documentation, choose *SAP NetWeaver* → *Administrator's Guide* → *SAP NetWeaver Security Guide*.
SAP NetWeaver documentation	**help.sap.com** → *Documentation* → *SAP NetWeaver*
SAP NetWeaver 2004s Installation Guide	**service.sap.com/installNW2004s**
SAP NetWeaver 2004s Usage Type Process Integration (PI) – Configuration Content	**help.sap.com** → *Documentation* → *SAP NetWeaver* → *Technology Consultant's Guide* → *Enabling Application-to-Application Processes* → *Configuration of Usage Type Process Integration (PI)*
SAP Supply Chain Management Documentation (SAP SCM Documentation)	**help.sap.com** → *Documentation* → *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 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 Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide* 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 (SAP AII) uses the mechanisms provided by the Application Server (ABAP), for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP AII, see the sections below. In addition, we provide a list of the standard users required for operating SAP AII.

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 AS (Java) and the Enterprise Portal. The UME also supports various persistency options, such as ABAP Engine or a directory server.
Application Server (Java) user management using the Visual Administrator	Use the Visual Administrator to maintain users and roles on the AS (Java). The 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 SAP Help Portal at **help.sap.com** under *SAP NetWeaver* → *SAP NetWeaver 2004s* → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *User Management*.

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 about user types, see User Types in the *SAP NetWeaver Application Server ABAP Security Guide*.

Standard Users

The table below shows the standard users or user groups that are necessary for operating SAP AII. It also includes some SAP NetWeaver and SAP Event Management (SAP EM) users or user groups.

Standard Users

System	User ID	Type	Password	Description
Application Server	<sapsid>adm	SAP System Administrator	To be entered	*SAP NetWeaver 2004s Installation Guide*
Application Server	SAPService <sapsid>	SAP System Service Administrator	To be entered	*SAP NetWeaver 2004s Installation Guide*
Application Server	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 According to Usage Types → Security Guides for the Usage Type AS → SAP NetWeaver Application Server ABAP Security Guide → User Authentication → Protecting Standard Users*
Application Server	SAP Standard 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 According to Usage Types → Security Guides for the Usage Type AS → SAP NetWeaver Application Server Java Security Guide → User Administration and Authentication → User Administration and Standard Users*
SAP Auto-ID Infrastructure	SAP AII User	Dialog user	To be entered	*Business Scenario Configuration Guide: RFID-Enabled Flexible Delivery Processing → User Administration → Users and Roles in SAP AII*
SAP Auto-ID	SAP AII	Service user	To be entered	*SAP Auto-ID 5.1:*

Infrastructure	WebDynpro Communication User			*Installation Guide → Installing SAP AII 5.1 → 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	Service user	To be entered	*SAP NetWeaver Installation Guide*
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 → SAP Event Management User*
SAP SCM WCL	SAP Event Management connection user	Communication user	To be entered	*SAP SCM Installation Guide: Installation/Upgrade Guide* – SAP WCL → *SAP SCM WAL – Specific Information → SAP SCM – WCL Configuration Parameters*
SAP ECC or SAP R/3	SAP backend Users	Dialog user	To be entered	*Business Scenario Configuration Guide: RFID-Enabled Outbound and Inbound Processing → User Administration → User Maintenance in ERP Systems and XI Systems*

For information on SAP NetWeaver standard users, see the SAP Help Portal at **`help.sap.com`** → *SAP NetWeaver → Administrator's Guide → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guides for the Usage Type AS → SAP NetWeaver Application Server ABAP Security Guide → User Authentication → Protecting Standard Users*.

For information on SAP NetWeaver password rules, see the SAP Help Portal at **help.sap.com** → *SAP NetWeaver* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *Authentication and Single Sign-On* → *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 (SAP AII) is based on SAP NetWeaver, all the mechanisms for user data synchronization of SAP NetWeaver are available for SAP AII.

We recommend that you configure the User Management Engine of the Java application so that it uses the ABAP user management of the SAP Web AS ABAP.

For information about user data synchronization, see SAP Help Portal at **help.sap.com** → *SAP NetWeaver* → *Administrator's Guide* → *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 (SAP AII) supports the Single Sign-On (SSO) mechanisms provided by the Application Server (Java and ABAP). Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide* and in the *SAP NetWeaver Application Server Java Security Guide* also apply to SAP AII. 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 about *Secure Network Communications (SNC)*, see the *SAP NetWeaver Security Guide*.

SAP logon tickets

SAP AII 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.

For more information about *SAP Logon Tickets,* see the *SAP NetWeaver 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.

For more information about *Client Certificates*, see the *SAP NetWeaver Security Guide*.

Authorizations

Use

SAP Auto-ID Infrastructure (SAP AII) uses the authorization provided by the Application Server (AS). Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to SAP AII.

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

Standard Roles

You can find standard roles in the profile generator using input help. You can use search terms to restrict the selection to the required standard roles, for example the search term *AIN* lists all SAP AII standard roles and the search term /SAPTRX* lists all SAP EM standard roles. The documentation of the role provides you with a detailed description of the role content.

For information about the standard roles in SAP AII, see the SAP Help Portal at help.sap.com → *mySAP Business Suite* → *SAP Auto-ID Infrastructure* → *Getting Started* → *Roles in SAP Auto-ID Infrastructure*.

For information on roles for AS and SAP EM, see the *SAP NetWeaver Security Guide* and the *SAP SCM Security Guide* on SAP Service Marketplace at **`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 5.1: Installation Guide* → *Installing SAP AII 5.1* → *Maintaining JCo Connections* → *Using Name/Password for Connection to Backend*.

Authorizations for Configuration in SAP ECC or SAP R/3

To configure the SAP ECC or SAP R/3 backend system, you can use the possibility to create IMG customizing roles.

For information about roles, see the SAP Help Portal at **`help.sap.com`** under *SAP NetWeaver* → *SAP NetWeaver by Key Capability* → *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*.

Roles in SAP Event Management

For information about roles in SAP Event Management (SAP EM), go to the SAP Help Portal at **help.sap.com** and choose *Documentation → SAP Business Suite → SAP Supply Chain Management → SAP SCM 5.1 → SAP Supply Chain Management (SAP SCM) → SAP Event Management (SAP EM) → Roles in SAP EM*.

For information about users and roles in SAP NetWeaver, go to the SAP Help Portal at **help.sap.com** → *Documentation → SAP NetWeaver → SAP NetWeaver 7.0 (2004s) → SAP Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → Security → Identify Management → Users and Roles (BC-SEC-USR)*.

Maintaining Authorizations for SAP Event Management

Use

Assigning Users to Scenarios

In SAP Event Management (SAP EM), you must assign users to scenarios. You can then specify that the system displays only the parameters and conditions that are relevant to that scenario.

Defining Authorization Profiles

In SAP EM, you also define authorization profiles to allow the following:

- Information to be displayed to query or evaluate event handler data
- Event handler to be created and changed in SAP EM

An authorization profile consists of one or more authorization profile parameter sets that the system uses to create the authorization parameters for an event handler. The authorization parameters determine how data is created, displayed, changed, or evaluated.

You assign an authorization profile to an event handler type to determine which event handlers are displayed to the user and which event handlers the user can change or create. The system displays all event handlers of an event handler type to the user. These types correspond to the control and information parameters of the user's authorization profile.

You create an authorization profile **Vendors Europe** with a control parameter **Vendor** and the value **Smith**. You assign the authorization profile to the event handler type **Vendors**. The vendor **Smith** can create, query, change, or evaluate all event handler data with the event handler type **Vendor**, the control parameter **Vendor**, and value **Smith**.

The system only checks the first forty characters of the parameter values.

Defining Filters and Assigning Filter Profiles to Users

By using filter profiles, you specify which event handler components the system displays to the user. You assign a filter profile to an event handler type and define different filter profiles for different event handler types. You can use this combination for one or more users.

You use roles to assign a user group to an existing filter profile, so that the appropriate event handler components are displayed to the user. You use the event handler type to assign the filter profile to a role.

Assigning Filter Profiles to Roles

You use roles to assign a user group to an existing filter profile, so that the appropriate event handler components are displayed to the user. You use the event handler type to assign the filter profile to a role.

Defining Event Message Senders

You define the senders who are authorized to send event messages to SAP EM.

Procedure

Assigning Users to Scenarios

1. In Customizing for SAP SCM, choose *Event Management* → *Solutions and Scenarios* → *Assign Users to Scenarios*.
2. Select a user name.
3. Assign the user to one of the scenarios predefined by SAP or to one of your own scenarios.

   You assign a user to all available scenarios by doing one of the following:

   - Entering an asterisk (*****)
   - Leaving the field blank

Defining Authorization Profiles

1. In Customizing for SAP SCM, choose *Event Management* → *Authorizations and Filters* → *Define Authorization Profiles*.
2. Define an authorization profile parameter set with the corresponding control or info parameters. Only the data that belongs to the parameters specified in this IMG activity is displayed to users when they create, change, query, or evaluate event handler data.

   

   You define the control and info parameters in Customizing for SAP SCM by choosing *Event Management* → *Event Handlers and Event Handler Data* → *Parameters* → *Define Control, Info, and Rule Processing Parameters*.
3. Define an authorization profile and assign one or more authorization profile parameter sets.
4. Specify an authorization group number for each authorization profile parameter set.

   When checking the authorization, the system checks whether a user is authorized for all parameters of an authorization group. If an event handler belongs to several authorization groups, the user needs authorization for only one of the groups to create, change, or display event handlers.
5. Assign the authorization profile to an event handler type.
6. In Customizing for SAP SCM, choose *SAP NetWeaver* → *Application Server* → *System administration* → *Users and Authorizations* → *Maintain Authorizations and Profiles Using Profile Generator* → *Maintain roles*
7. Assign the authorization profile to a role.

For more information about users and roles, go to the SAP Help Portal at **`help.sap.com`** and choose *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 7.0 (2004s)* → *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *Users and Roles (BC-SEC-USR)*.

Defining Filters Profiles and Assigning Filter Profiles to Users

1. In Customizing for SAP SCM, to:
2. Define filter profiles, choose *Event Management* → *Authorizations and Filters* → *Define Filter Profiles.*
3. Assign filter profiles to users, choose *Event Management* → *Authorizations and Filters* → *Assign Filter Profiles to Users*.
4. Select the user name.
5. Create a new entry for the corresponding event handler type and the corresponding filter profile.

   The filter profile determines the filtering of data about event handlers belonging to the selected event handler type, which the system displays.

Assigning Filter Profiles to Roles

1. In Customizing for SAP SCM, choose *Event Management* → *Authorizations and Filters* → *Assign Filter Profiles to Roles*.
2. In the dialog box, specify a user role for the work area.
   - To enable selection based on the event handler type or filter profile, choose *Further select cond.* → *Continue*.
   - If required, add entry lines, change the order of the entry lines, or reset the previous entries by making a new selection.
3. Create a new entry for the corresponding event handler type and filter profile.

   The filter profile filters the data that the system displays to event handlers of the selected type.

   

   Before you can assign filter profiles to roles, you have to define them in Customizing for SAP SCM (see *Defining Filter Profiles and Assigning Filter Profiles to Users* above).

Defining Event Message Senders

1. In Customizing for SAP SCM, choose *Event Management* → *Authorizations and Filters* → *Define Event Message Senders*.
2. Define the senders who are authorized to send event messages to SAP EM.

   

   This table is not user-dependent.
3. Enter the sender code set and the sender code ID.

   For example, you can enter **`US`** for user as the code set and **`TEST_SMITH`** as the code ID.

Sender Transaction	Code Set	Code ID
Web Interface	WCL	<User Name>
External Entry (for example, BAPI, IDoc)	Any	Any

4. In the table, the system checks whether an authorization exists to send an event message in the following sequence:
   a. Is the sender authorized to send an event message to SAP EM?
      - If an appropriate entry is found, the system forwards the event message to SAP EM and assigns it to the corresponding event handler.

- If an appropriate entry is not found, the system continues to check the authorization for the user who is logged on.

b. Has the authorization to send an event message to SAP EM been set up in the user master that belongs to the user who is currently logged on?

- If the authorization check is successful, the system forwards the event message to SAP EM and assigns it to the corresponding event handler.
- If the authorization check is not successful, the system sends the event message, and an appropriate error message, to the sender.

For more information on creating and maintaining authorizations, go to the SAP Help Portal at **`help.sap.com`** and choose *Documentation* → *SAP NetWeaver* → *SAP NetWeaver 7.0 (2004s)* → *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *Security* → *Identity Management* → *Users and Roles (BC-SEC-USR).*

In this Customizing activity, you can define all new users who are authorized to send an event message, but do not assign them an authorization to send event messages in the user master

This option is useful to:

- Authorize certain users to manually (online) create event messages using the Web interface
- Restrict external senders who are simultaneously using automatic background programs to report events

The table for setting up authorizations is user-dependent.

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 Guides for Connectivity and Interoperability Technologies*

Communication Channel Security for SAP AII

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 (SAP AII) to achieve a secure system landscape.

For information on the communication security of SAP NetWeaver, see SAP Help Portal at **`help.sap.com`** → *SAP NetWeaver* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

For information on security aspects for connectivity and interoperability of SAP NetWeaver, see SAP Help Portal at **`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver Security Guide* → *Security Guides for Connectivity and Interoperability Technologies.*

As SAP AII 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 on mobile devices within SAP Auto-ID Infrastructure, see the SAP Help Portal at **`help.sap.com`** → *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Auto-ID Infrastructure* → *Data Management* → *Master Data* → *RFID Device*.

The table below shows the communication paths used by SAP AII, 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	For example passwords, business data
Front end client using a Web browser to application server	HTTP(S)	All application data	For example 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	For example passwords, business data

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

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 NetWeaver Usage Type Process Integration for the integration of SAP Auto-ID Infrastructure, consult also the *SAP NetWeaver Security Guide.*

Communication Channel Security for SAP EM and SAP SCM - WCL

SAP Event Management (SAP EM)

Since SAP EM comes with interfaces to connect application systems, internal and external systems and devices, and a data warehouse system, a special focus on the communication channel security is necessary. SAP recommends that you activate a secure communication protocol for all communication channels used (for example, SNC), especially if you use mobile devices to connect to SAP EM.

For more information about the infrastructure of SAP EM, go to the SAP Help Portal at **help.sap.com** and choose *SAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 5.1* → *SAP Supply Chain Management (SAP SCM)* → *SAP Event Management (SAP EM)* → *SAP Event Management Infrastructure* → *Application Integration*.

Since several interfaces of SAP EM are available to connect to SAP NetWeaver Exchange Infrastructure (SAP NetWeaver XI), SAP recommend that you consult the SAP NetWeaver XI Security Guide.

For more information about the infrastructure of SAP EM, go to the SAP Help Portal at **help.sap.com** and choose *SAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 5.1* → *SAP Supply Chain Management (SAP SCM)* → *SAP Event Management (SAP EM)* → *System Installation and Integration* → *SAP Exchange Infrastructure Integration*.

You can find the SAP NetWeaver XI security guide on the SAP Service Marketplace at **service.sap.com/security** → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *Security in Detail* → *SAP Security Guides* → *SAP Process Integration (PI) Security Guides* → *SAP Exchange Infrastructure (XI) Security Guide*.

Since you can assign an URL as a link to a configured field in Customizing for SAP EM, you are responsible for the content and security of this URL. SAP recommend that you use the SAP Web Repository. You can check documents or graphics before they are uploaded and use a virus scan.

SAP SCM - Web Communication Layer (SAP SCM - WCL)

SAP recommends that you use Secure Socket Layer (SSL), since the ERP user and its password are used to log onto SAP SCM - WCL.

For more information about security recommendations in SAP SCM - WCL, see the SAP J2EE Engine documentation installation guide, at **`service.sap.com/instguides`** → *SAP Components* → *SAP Solutions for RFID* → *Using SAP Auto-ID Infrastructure 2007* → *SAP Event Management - Web Communication Layer 5.1.*

For more information about Web Dynpro, go to the SAP Help Portal at **`help.sap.com`** and choose *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Aspects for Usage Type DI and Other Development Technologies* → *Security Issues in Web Dynpro for ABAP.*

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, see SAP Help Portal at **`help.sap.com`** → *SAP NetWeaver* → *Administrator's Guide* → *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 on access control using firewalls, see SAP Help Portal at **`help.sap.com`** → *SAP NetWeaver* → *Administrator's Guide* → *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 (SAP AII). To give a better overview the communication destinations for the XI system, 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 5.1: Installation Guide → *Installing SAP AII 5.1* → *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 5.1: Installation Guide → *Installing SAP AII 5.1* → *Maintaining JCo Connections*

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

Description	SAP Auto-ID Infrastructure Documentation → *Integration* **and** *RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in SAP Auto-ID Infrastructure → Setting Up RFC Destinations from SAP AII to the XI System* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment / Creating RFC Destinations in the ABAP and Java Environments* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

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

Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the XI System → Maintaining the System Landscape Directory (SLD)* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment / Creating RFC Destinations in the ABAP and Java Environments* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

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

Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the XI System → Maintaining the System Landscape Directory (SLD)* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment / Creating RFC Destinations in the ABAP and Java Environments* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

Destination	SAP AII → RFID devices / RFID device controller
Delivered	No
Type	HTTP
User, Authorizations	-
Description	SAP Auto-ID Infrastructure Documentation → *Integration* **and** *RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in SAP Auto-ID Infrastructure → Maintaining Device Settings* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

Destination	XI System → SAP AII
Delivered	No
Type	RFC - HTTP

User, Authorizations	-
Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in SAP Auto-ID Infrastructure → Setting up RFC Destinations from SAP AII to the XI System* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

Destination	XI System → XI System <LCRSAPRFC>
Delivered	No
Type	RFC – TCP/IP
User, Authorizations	-
Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the XI System→ Maintaining the System Landscape Directory (SLD)* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP and Java Environments*

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

Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the XI System → Maintaining the System Landscape Directory (SLD)* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP and Java Environments*

Destination	XI System → SAP ECC or SAP R/3
Delivered	No
Type	RFC- ABAP Connection
User, Authorizations	See references
Description	SAP Auto-ID Infrastructure Documentation → *Integration* **and** *RFID–Enabled Outbound Processing Configuration Guide → Settings in the XI System → Setting Up RFC Destinations from the XI System to an ERP System* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Integration of Business Systems → Integration using the IDoc Adapter*

Destination	SAP EM → SAP ECC or SAP R/3
Delivered	No
Type	RFC – ABAP Connection
User, Authorizations	Use the Profile Generator (transaction **PFCG**) to define an appropriate profile

Description	*RFID-Enabled Delivery Processing Configuration Guide → Settings in the ERP System → Settings in the ERP System for Integration with SAP SCM → Setting Up RFC Destinations from the Application System to SAP SCM* **and** SAP SCM Documentation → *SAP Event Management (SAP EM) → System Installation and Integration* **and** SAP EM IMG: *Event Management → General Settings in SAP Event Management → Define RFC Connection to Application System*.

Destination	SAP ECC or SAP R/3 → XI System
Delivered	No
Type	RFC – ABAP Connection
User, Authorizations	User role: SAP_XI_APPL_SERV_USER
Description	SAP Auto-ID Infrastructure Documentation → *Integration* **and** *RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the ERP System → Communication Settings (Outbound Processing) → Setting Up RFC Destinations from the ERP System to the XI System* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Communication and Security → User Management and User Roles* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Integration of Business Systems → Integration using the IDoc Adapter*

Destination	SAP ECC or SAP R/3 → XI System <SAPSLDAPI>
Delivered	No
Type	RFC - TCP/IP
User, Authorizations	-
Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the XI System → Maintaining the System Landscape Directory (SLD)* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment / Creating RFC Destinations in the ABAP and Java Environments* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

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

Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the XI System→ Maintaining the System Landscape Directory (SLD)* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Template-Based Basic Configuration → Creating RFC Destinations in the ABAP Environment / Creating RFC Destinations in the ABAP and Java Environments* **and** SAP NetWeaver Documentation → *Technology Consultant's Guide → Enabling Application-to-Application Processes → Application-to-Application Integration → Configuration of Usage Type Process Integration (PI) → Configuration of Business Systems with an Integration Engine*

Destination	SAP ECC or SAP R/3 → SAP EM
Delivered	No
Type	RFC – ABAP Connection
User, Authorizations	Use the Profile Generator (transaction **PFCG**) to define an appropriate profile
Description	*RFID-Enabled Flexible Delivery Processing: Configuration Guide→ Settings in the ERP System → Settings in the ERP System for Integration with SAP SCM → Setting Up RFC Destinations from the Application System to SAP SCM* **and** SAP SCM Documentation → *SAP Event Management (SAP EM) → System Installation and Integration*

SAP EM and XI connections are only relevant if you implement SAP EM and 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 SAP Help Portal at **help.sap.com** → *SAP NetWeaver* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guides for the Operation System and Database Platforms*.

Data Storage Security for SAP SCM - WCL

Logging Manager Parameters

The SAP SCM – Web Communication Layer (SAP SCM – WCL) uses the Logging Application Programming Interface (API), and the Logging Manager parameters configure the API. The logging file and pattern is set with the following parameters:

- `Log File ID`
- `Log File Pattern`

You must protect the folder in which the log file is located on your server from unauthorized, third-party access.

Security for Additional Applications

Use

You can integrate SAP Auto-ID Infrastructure (SAP AII) with any RFID device controllers or fixed RFID devices that support HTTP communication. Since these 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 18] and SAP Help Portal at **help.sap.com** under *mySAP Business Suite* → *mySAP Supply Chain Management* → *SAP Auto-ID Infrastructure* → *Data Management* → *Master Data* → *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. However, SAP AII does support security for communicating with device controllers and mobile devices via HTTPS to obscure the content of messages being transmitted. For more information about security via HTTPS, see Communication Channel Security [Page 18].

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 SAP Service Marketplace at **`service.sap.com/webdynpro`.**

Auditing and Logging

SAP systems keep a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Audits and logs are important for monitoring the security of your system and to track events, in case of problems. All trace and log files of SAP Auto-ID Infrastructure use SAP NetWeaver standard mechanisms.

For information about auditing and logging, see the security guide for SAP NetWeaver 2004s under **`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver 2004s* → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide*.

Minimal Installation SAP SCM - WCL and SAP EM

Since the SAP SCM - Web Communication Layer (WCL) interface is Java-based, you might have some functional restrictions in the event of calling the function modul via the SAP Java Connector (SAP JCo) in the backend.

For more information about the SAP EM Web interface, see SAP SCM Documentation at **`help.sap.com`** → *Documentation* → *SAP Business Suite* → *SAP Supply Chain Management* → *SAP SCM 5.1* → *English* → *SAP Supply Chain Management (SAP SCM)* → *SAP Event Management (SAP EM)* → *SAP Event Management Infrastructure* → *User Interfaces*.

For more information about the SAP JCo, see the SAP JCo documentation at **`help.sap.com`** → *Documentation* → SAP NetWeaver → *SAP NetWeaver 7.0 (2004s)* → *English* → *SAP Library* → *SAP NetWeaverLibrary* → *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using Java* → *Core Development Tasks* → *Connectivity and Interoperability* → *SAP Java Connector.*

`help.sap.com` → *Documentation* → SAP NetWeaver → *SAP NetWeaver 7.0 (2004s)* → *English* → *SAP Library* → *SAP NetWeaverLibrar* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Aspects for System Management* → *Security Guide for the SAP System Landscape Directory.*