SAP Credit Management
Security Guide



Release 6.05

Copyright

© Copyright 2010 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.
Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, Clear Enterprise, SAP BusinessObjects Explorer and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP France in the United States and in other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or

omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
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`.

Contents

SAP Credit Management Security Guide 5
Introduction 5
Before You Start 7
Technical System Landscape 8
Security Aspects of Data, Data Flow and Processes 10
User Administration and Authentication 11
User Management 11
Integration into Single Sign-On Environments 12
Authorizations 13
Defining Authorizations 13
Session Security Protection 15
Network and Communication Security 15
Communication Channel Security 16
Network Security 17
Communication Destinations 18
Data Storage Security 18
Enterprise Services Security 19
Security-Relevant Logging and Tracing 19
Services for Security Lifecycle Management 19

Introduction



This guide does not replace the administration or operation guides that are available for productive operations.

Target Audience

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to *SAP Credit Management*. To assist you in securing *SAP Credit Management*, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to *SAP Credit Management*.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**

  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that form the foundation for this Security Guide.

- **Technical System Landscape**

  This section provides an overview of the technical components and communication channels that are used by *SAP Credit Management*.

- **Security Aspects of Data, Data Flow and Processes**

  This section provides an overview of security aspects involved throughout the most-widely used processes within *SAP Credit Management*.

- **User Management and Authentication**

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

  - Recommended tools to use for user management.
  - User types that are required by *SAP Credit Management*.
  - Standard users that are delivered with *SAP Credit Management*.
  - Overview of the user synchronization strategy if several components or products are involved.
  - Overview of how integration into Single Sign-On environments is possible.

- **Authorizations**

  This section provides an overview of the authorization concept that applies to *SAP Credit Management*.

- **Session Security Protection**

  This section provides information about activating secure session management, which prevents javascript or plug-ins from accessing the SAP logon ticket or security session cookie(s).

- **Network and Communication Security**

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

- **Data Storage Security**

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

- **Enterprise Services Security**

  This section provides an overview of the security aspects that apply to the enterprise services delivered with *SAP Credit Management*.

- **Security-Relevant Logging and Tracing**

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

- **Services for Security Lifecycle Management**

  This section provides an overview of services provided by Active Global Support that are available to assist you in maintaining security in your SAP systems on an ongoing basis.

Before You Start

Fundamental Security Guides

SAP Credit Management is based on the *SAP Netweaver* technology. Therefore, the corresponding Security Guides also apply to *SAP Credit Management*. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Fundamental Security Guides

Scenario, Application, or Component Security Guide
SAP Netweaver Security Guide
SAP Exchange Infrastructure Security Guides
SAP Enterprise Portal Security Guides
SAP Business Information Warehouse Security Guides

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

Important SAP Notes

For a list of security-relevant SAP Hot News and SAP Notes, see *SAP Service Marketplace* at `http://service.sap.com/securitynotes`.

Configuration

There is a configuration guide available for *SAP Credit Management*. You can find it on *SAP Service Marketplace* at **`http://service.sap.com/fscm`** → *SAP Credit Management* → *Media Library*.

It contains, amongst other things, information about the following subjects:

- System Connections
- Process Integration with SAP Systems

Additional Information

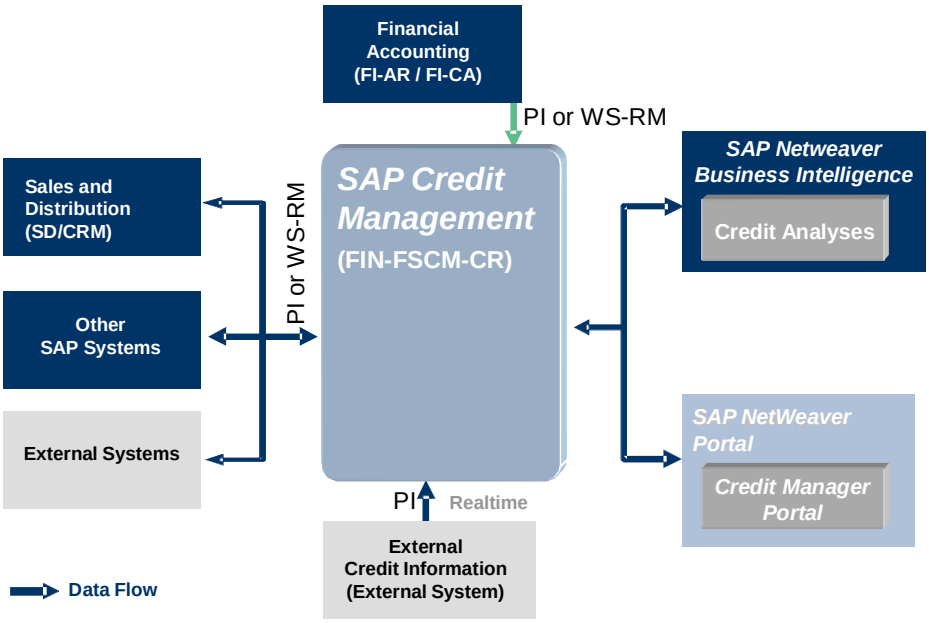
For more information about specific topics, see the sources shown in the table below.

Content	Quick Link on SAP Service Marketplace or SDN
Security	**`http://sdn.sap.com/irj/sdn/security`**
Security Guides	**`http://service.sap.com/securityguide`**
Related SAP Notes	**`http://service.sap.com/notes`** **`http://service.sap.com/securitynotes`**
Released platforms	**`http://service.sap.com/pam`**
Network security	**`http://service.sap.com/securityguide`**
SAP Solution Manager	**`http://service.sap.com/solutionmanager`**
SAP NetWeaver	**`http://sdn.sap.com/irj/sdn/netweaver`**

Technical System Landscape

Use

The figure below shows an overview of the technical system landscape for *SAP Credit Management*.



To exchange messages with external information providers, you have to use the *Integration Server.* For accounting systems as well as *Sales and Distribution* (SD) systems, you can configure the communication either via the *Integration Server* or via a point to point connection using *Web Services Reliable Messaging* (WS-RM). The *SAP Business Information Warehouse* is connected via *Remote Function Call* (RFC).

For more information about recommended security zone settings, see *SAP NetWeaver '04 Security Guide (Complete)* on *SAP Service Marketplace* at **`service.sap.com/securityguide`**.

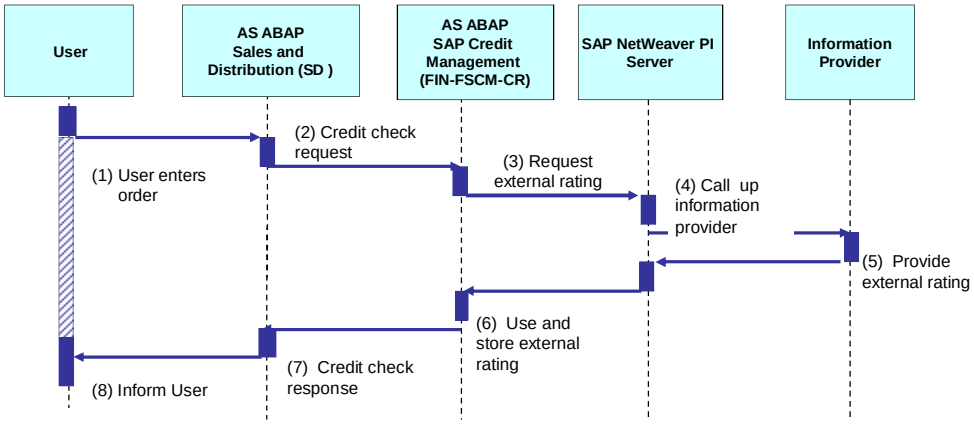
For *SAP Credit Management* the Business Package for the Credit Manager provides you with portal content so that you can use the functions from *SAP Credit Management* in the portal. Security-relevant information about the use of the portal content is available in the *SAP NetWeaver Security Guide* for the usage types Enterprise Portal Core (EPC) and Enterprise Portal (EP) in the portal Security Guide.

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

Content	Guide/Tool	Quick Link on SAP Service Marketplace or SDN
Technical description for *SAP Credit Management* and the underlying components such as *SAP NetWeaver*	*Master Guide*	**http://service.sap.com/instguides**
High availability	*High Availability for SAP Solutions*	**http://sdn.sap.com/irj/sdn/ha**
Technical landscape design	See applicable documents	**http://sdn.sap.com/irj/sdn/landscapedesign**
Security	See applicable documents	**http://sdn.sap.com/irj/sdn/security**

Security Aspects of Data, Data Flow and Processes

The figure below shows an example of a data flow for the *SAP Credit Management* application.



The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	User enters order	User types: dialog or Internet user
2	Credit check request	Communication protocol HTTPS or HTTP
3	Request external rating	Communication protocol HTTPS or HTTP
4	Call up information provider	Communication protocol HTTPS or HTTP,
5	Provide external rating	not applicable
6	Use and store external rating	not applicable
7	Credit check response	Communication protocol HTTPS or HTTP
8	Inform user	not applicable

User Administration and Authentication

SAP Credit Management uses the user management and authentication mechanisms provided with the *SAP NetWeaver* platform, in particular the *SAP NetWeaver Application Server for ABAP*. Therefore, the security recommendations and guidelines for user management and authentication as described in the SAP NetWeaver Application Server Security Guide for ABAP Technology [SAP Library] also apply to *SAP Credit Management*.

In addition to these guidelines, we include information about user management and authentication that specifically applies to *SAP Credit Management* in the following topics:

- User Management [Page 11]

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with *SAP Credit Management*.

- Integration Into Single Sign-On Environments [Page 12]

  This topic describes how *SAP Credit Management* supports Single Sign-On mechanisms.

User Management

Use

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

To use the content in the portal, you need to have a portal user. The user defined in the *ERP* system must be assigned to the portal. You can do this by logging on with single sign-on or with user mapping.

User Management Tools

The table below shows the tools to use for user management and user administration with *SAP Credit Management*.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance with *SAP NetWeaver AS ABAP* (Transactions SU01, PFCG)	For more information, see Users and Roles (BC-SEC-USR) [SAP Library].	

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.

The user types that are required for *SAP Credit Management* include:

- Individual users:
  - Dialog users are used for SAP GUI for Windows connections
- Technical users:
  - Communication users are used for PI communication.

For more information on these user types, see User Types [SAP Library] in the *SAP NetWeaver Application Server for ABAP* Security Guide.

Standard Users

The table below shows the standard users that are necessary for operating *SAP Credit Management*.

Standard Users

System	User ID	Type	Password	Description
Credit Management, client systems	e.g. CREDITXIUSER	communication user	You specify the initial password during the installation. The user ID and password are stored in the XI-Channel for the connection.	This is required for communication between *SAP Credit Management* and client systems using the XI Channel.

You need to create this user before XI configuration. Assign both roles SAP_FIN_FSCM_CR_USER and SAP_XI_IS_SERV_USER to the user. The user and password are added to the XI Channel logon data that you create when you configure your exchange server.

Integration into Single Sign-On Environments

Use

SAP Credit Management supports the Single Sign-On (SSO) mechanisms provided by *SAP NetWeaver Application Server for ABAP*. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server Security Guide [SAP Library] also apply to *SAP Credit Management*.

For more information, about the available authentication mechanisms, see User Authentication and Single Sign-On [External] in the *SAP NetWeaver Library*.

Authorizations

Use

SAP Credit Management uses the authorization provided by the *SAP NetWeaver Application Server*. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server Security Guide for ABAP* also apply to *SAP Credit Management*.

The *SAP NetWeaver Application Server* authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the *SAP NetWeaver Application Server for ABAP* and the *User Management Engine's* user administration console for *SAP NetWeaver Application Server for Java*.



For more information about how to create roles, see Role Administration

Standard Roles

The table below shows the standard roles that are used by *SAP Credit Management*.

Standard Roles

Role	Description
SAP_FIN_FSCM_CR_USER	Credit Management - Credit Analyst
SAP_XI_IS_SERV_USER	Exchange Infrastructure: Integration Server Service User

The authorization objects for role SAP_FIN_FSCM_CR_USER are described in the following section (also included in the *SAP Credit Management Configuration Guide*).

Defining Authorizations

Use

You can control the right of access to *SAP Credit Management* data by assigning authorizations – separately by credit segment and activity - to the authorization object F_UKM_SGMT. The fields of this authorization object are:

- Credit Segment
- Activity, with the definitions
  - 01 Add or create
  - 02 Change
  - 03 Display
  - 06 Delete
  - 08 Display Change Documents
  - 43 Release

The role SAP_FIN_FSCM_CR_USER is delivered with all authorizations to this authorization object.

You can restrict the access to credit segment-independent master data of *SAP Credit Management* (for example, the score) by using the authorization object for business partner roles (B_BUPA_RLT) with the role *Business Partner Credit Management* (UKM000).

You can restrict the access to logs (application logs) of *SAP Credit Management* using the authorization object S_APPL_LOG. The fields of this authorization object are:

- Application Log Object Name
- Application Log Subobject
- Activity, with the definitions
    - 03 Display
    - 06 Delete

For *SAP Credit Management*, the following forms are relevant for object name and subobject:

Object Name	**Subobject**	**Meaning**
FIN-FSCM-CR	BW-SCORING	Transfer of score from BW
FIN-FSCM-CR	COMMITMENT	Credit exposure update
FIN-FSCM-CR	CREDITCHECK	Credit check
FIN-FSCM-CR	MONITOR	Update entries for external credit Information
FIN-FSCM-CR	SEARCH_ID	Search ID at credit information provider
FIN-FSCM-CR	REPLICATE	Replicate FI-CA score
FIN-FSCM-CR	EVENTING	Log of events ocurred
FIN-FSCM-CR-MASS	ERROR, ERROR_BIG, ERROR_PROG, ERROR_UPD, INFO, STATISTICS, SUCCESS, WARNING	Logs of mass changes, can be differentiated by the severity of the error

Procedure

You can organize the authorizations of your users as follows:

Activities	Authorization	Activity
Restrict access to one or more credit segments	F_UKM_SGMT with specified credit segment	
Edit master data	F_UKM_SGMT	01 02 03
Display master data	F_UKM_SGMT	03
Delete master data	F_UKM_SGMT	06
Display change documents for master data changes	F_UKM_SGMT	08
Release and reject credit limit changes/increases requested (dual control principle)	F_UKM_SGMT	43
Edit and display master data of *SAP Credit Management*	B_BUPA_RLT with the business partner role UKM000	
Display and/or delete application logs of *SAP Credit Management*	S_APPL_LOG with the object names and subobjects listed above	03 06

Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection on the AS ABAP

To activate session security on the AS ABAP, set the corresponding profile parameters and activate the session security for the client(s) using the transaction SICF_SESSIONS.

For more information, a list of the relevant profile parameters, and detailed instructions, see Activating HTTP Security Session Management on AS ABAP.

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 Credit Management* 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 Credit Management*. Details that specifically apply to *SAP Credit Management* are described in the following topics:

- Communication Channel Security [Page 16]

  This topic describes the communication channels and protocols used by *SAP Credit Management*.

- Network Security [Page 17]

  This topic describes the recommended network topology for *SAP Credit Management*. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate *SAP Credit Management*.

- Communication Destinations [Page 17]

  This topic describes the information needed for the various communication channels, for example, which users are used for which communications.

For more information, see the following sections in the *SAP NetWeaver* Security Guide:

- Network and Communication Security [SAP Library]
- Security Aspects for Connectivity and Interoperability [SAP Library]



Communication Channel Security

Use

The table below shows the communication channels used by *SAP Credit Management*, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Frontend client using SAP GUI for Windows to application server	DIAG	All application data	Passwords
Application server to application server	RFC	All application data	
Application server to external credit agency	HTTPS	Business partner ID, credit ratings	Credit ratings

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.



We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see Transport Layer Security [SAP Library] in the *SAP NetWeaver* Security Guide.

Network Security

Use

All the components described under Technical System Landscape [Page 7] can be found in a typical configuration of *SAP Credit Management*, apart from the external credit information providers in the DMZ and server LAN zones. The credit information providers are external partners located outside the firewall in the Internet zone.

For more information on the network configuration of an SAP Exchange Infrastructure installation, see Network Zones [SAP Library] in the SAP Security Guide XI and Using Multiple Network Zones [SAP Library] in the *SAP NetWeaver* Security Guide.

For more information about the services and ports used by *SAP NetWeaver*, see Network Services [SAP Library] in the *SAP NetWeaver* Security Guide.

For more information on firewall installations, see Using Firewall Systems for Access Control [SAP Library] in the *SAP NetWeaver* Security Guide.

Ports

SAP Credit Management runs on *SAP NetWeaver* and uses the ports from the AS ABAP. For more information, see the topic for AS ABAP Ports [External] in the corresponding *SAP NetWeaver Security Guide*. For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, also see the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Developer Network at **`http://sdn.sap.com/irj/sdn/security`** under *Infrastructure Security* → *Network and Communications Security*.

Communication Destinations

Use

The table below shows an overview of the communication destinations used by *SAP Credit Management*.

Connection Destinations when Using the Integration Server

Destination	Delivered	Type	User, Authorizations	Reference
INTEGRATION_SERVER	No	RFC	XIAPPLUSER Role SAP_XI_APPL_SERV_USER	service.sap.com /instguides → SAP NetWeaver Configuration Guide SAP XI 7.0 or higher
LCRSAPRFC	No	RFC		service.sap.com /instguides → SAP NetWeaver Installation Guide SAP Exchange Infrastructure 7.0 or higher
SAPSLDAPI	No	RFC		service.sap.com /instguides → SAP NetWeaver Installation Guide SAP Exchange Infrastructure 7.0 or higher

These destinations are not application-specific but they are required for the operation of the Exchange Infrastructure.

For point to point connections via *Web Services Reliable Messaging* (WS-RM), you use the *SOA Manager* in both systems to create the logical port and the endpoint.

Data Storage Security

Use

Master and transaction data of *SAP Credit Management* are saved in the database of the SAP system in which *SAP Credit Management* is installed. They are not distributed to connected systems via XI, however they can be optionally extracted to *SAP Business Information Warehouse*.

Access to this data is restricted through the authorizations for authorization object F_UKM_SGMT. Authorizations for this authorization object are provided for role SAP_FIN_FSCM_CR_USER in the standard delivery; you can copy the role and adapt it as required. For more information on authorization object F_UKM_SGMT, see the configuration guide of *Credit Management*.

Access to data on natural persons in particular is subject to data protection requirements and must be restricted by assigning authorizations.

Enterprise Services Security

The following chapters in the NetWeaver Security Guide and documentation are relevant for all enterprise services delivered with the *SAP Credit Management* application:

- Security Guide Web Services [External]
- Recommended WS Security Scenarios [External]
- SAP NetWeaver Process Integration Security Guide [External]

Security-Relevant Logging and Tracing

Use

All changes to the master data of *SAP Credit Management* are recorded as change documents in the business partner record. Changes automatically executed by the system as a follow-on process to an event appear under the name of the communication user if the event was triggered by an XI message. (Example: A credit check is initiated by SD; the system detects that the validity date of the credit limit has expired and determines a new credit limit on the basis of the Customizing settings.)

For more information, see the *SAP NetWeaver Security Guide* at **`http://service.sap.com/securityguide`** → Auditing and Logging.

Services for Security Lifecycle Management

The following services are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWarch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.

  In this case, analyze and implement the identified notes, if possible. If you cannot implement the notes, the report should be able to help you decide on how to handle the individual cases.

- Whether an accumulation of critical basis authorizations has been identified.

  In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.

- Whether standard users with default passwords have been identified on your system.

  In this case, change the corresponding passwords to non-default values.

Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security relevant configuration parameters
- Critical users
- Missing security patches.

This service is available as a self service within the SAP Solution Manager or as a remote or on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation of a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continously monitor a system landscape for compliance to predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existance of a non-trivial Gateway configuration or making sure standard users do not have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

More Information

For more details on these services see

- EarlyWatch Alert: **`http://service.sap.com/ewa`**
- Security Optimization Service / Security Notes Report: **`http://service.sap.com/sos`**
- Comprehensive list of Security Notes: **`http://service.sap.com/securitynotes`**
- Configuration Validation: **`http://service.sap.com/changecontrol`**
- RunSAP Roadmap, including the Security and the Secure Operations Standard: **`http://service.sap.com/runsap`** (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)