Security Guide

Document version: 1.4 – 2015-07-13

CUSTOMER

SAP Customer Relationship Management

SAP enhancement package 3 for SAP CRM 7.0

Document History

⚠ Caution

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version on SAP Service Marketplace at service.sap.com/securityguide ↗ .

The following table provides an overview of the most important document changes:

Table 1

Version	Date	Description
1.0	2013-08-13	Initial version
1.1	2013-12-05	Reference to security information for SAP Fiori apps added to the *Before You Start* section
1.2	2014-07-18	SAP enhancement package 3 (SP05) for SAP CRM 7.0: • *Data Protection* section added • Data protection information added to the *Utilities: B2C Call Center and B2B Work Center* section • Data protection information added to the *SAP Social Services Management for Public Sector* section • Information about text message integration and social media integration added to the *Component-Specific Guidelines: Interaction Center* section • Data storage security information added to the *Sales and Order Management* section
1.3	2015-01-29	SAP enhancement package 3 (SP07) for SAP CRM 7.0: Provider contract added to the list of business transactions in the WebClient UI that are relevant for payment card data (*Payment Card Security According to PCI-DSS* section)
1.4	2015-07-13	SAP enhancement package 3 (SP09) for SAP CRM 7.0: Information about payment on request feature added to the *SAP Social Services Management for Public Sector* section

Content

1 Introduction

Caution

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

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 certain phases of the software life cycle, whereas the security guide provides information that is relevant for all the phases of the software life cycle.

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 Customer Relationship Management (SAP CRM), since important business data and personal information are processed and stored by SAP CRM.

SAP CRM enables you to collaborate with your in-house and field employees, and with your partners and customers. Therefore, the components of SAP CRM access multiple data sources and business processes on behalf of different users holding different roles and they require different levels of security. To meet your specific business needs, SAP CRM allows you to use various access options.

Access to the data in SAP CRM must be granted only for authorized users. Unfortunately, a unique and uniform security implementation that suits all possible usage scenarios does not exist. Therefore, SAP CRM provides you with flexible and configurable security mechanisms, which allow you to implement the necessary security restrictions according to your requirements.

Example

SAP CRM, typically, contains and provides access to the following type of data:

- User master data, representing personal data that must also be protected by law in several countries
- Dynamic data created by users or by transaction processing, representing your core business data:
  - Account and contact information or credit card data of customers
  - Information about opportunities, forecasts, campaigns, or marketing plans
  - Pricing information of products, offers, contracts, and conditions

Depending on the scenario (see Technical System Landscape [page 9]), the information must be protected at different levels by using different protection mechanisms.

Note that the information is available not only through the SAP CRM functions, but also at technical levels (for example, the network), if not appropriately secured.

To understand the importance of correct security configuration, consider the following scenarios when using any SAP CRM solution:

- Due to an incorrect configuration in the access restrictions, an administrative interface can be accessed from the Internet. Attackers have recognized the weakness and, after appropriate changes using the administration functions, can access data of other users.

- A laptop of a field sales representative has been stolen. Unfortunately, the local information store holding SAP CRM information has not been secured; it contains all information about your offer concerning a large-volume contract for which your company is competing with several other companies. A competing company gets this information, adjusts its offer appropriately, and wins the contract.

Protecting your data using appropriate security configuration can be crucial for the success of your business.

About This Document

In this security guide, the *Introduction* section details the security recommendations for SAP CRM. Subsequent sections detail the steps specific to the relevant application or component. In some cases, such steps may deviate from the guidelines in the *Introduction* section.

> i Note
>
> You must take into account both the Introduction section and the section dedicated to your application or component.

1.1 Before You Start

Fundamental Security Guides

SAP Customer Relationship Management (SAP CRM) is built on top of several standard SAP components and can be integrated with several components. Therefore, the corresponding security guides are also relevant for SAP CRM, as applicable:

- SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP
- SAP NetWeaver AS JAVA
- SAP Content Server
- SAP TREX
- SAP NetWeaver Business Warehouse (SAP NetWeaver BW)
- SAP NetWeaver Mobile
- SAP NetWeaver Process Integration (SAP NetWeaver PI)

  For information on the appropriate SAP NetWeaver PI release, see SAP Note 1515223.
- SAP ERP
- SAP Biller Direct
- SAP Credit Management
- SAP Advanced Planning & Optimization (SAP APO)
- SAP Web Channel Experience Management
- SAP Master Data Governance
- SAP HANA (only relevant if SAP HANA is your primary or secondary database)
- SAP Fiori

  For information regarding SAP Fiori apps, see SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose relevant release>* › *SAP Fiori for SAP CRM*.

Additional Information

Table 2

Content	Quick Link on SAP Service Marketplace
SAP CRM	service.sap.com/crm
SAP CRM installation and upgrade	service.sap.com/crm-inst
Security	service.sap.com/security
Security guides	service.sap.com/securityguide
Security guides for SAP HANA (only relevant if SAP HANA is your primary or secondary database)	help.sap.com/hana_appliance
Security-relevant SAP hot news and SAP Notes	service.sap.com/securitynotes
SAP Notes	service.sap.com/notes
Released platforms	service.sap.com/platforms
SAP Solution Manager	service.sap.com/solutionmanager

1.2 Overview of SAP CRM Scenarios

For more information, see SAP Solution Manager.

1.3 Technical System Landscape

Security depends not only on correct configuration of each of the SAP Customer Relationship Management (SAP CRM) components, but also on the technical system landscape:

- Which technical components must be installed?
- Where are the technical components located in the network?
- Which communication links must be considered?
- What kinds of protocols are used over the communication links?
- What access paths are necessary and how are they realized technically?

> Note
>
> There is no single typical system landscape for SAP CRM. The system landscape depends on the key capabilities and scenarios that you use.

The following figure shows an overview of the technical system landscape for SAP CRM:

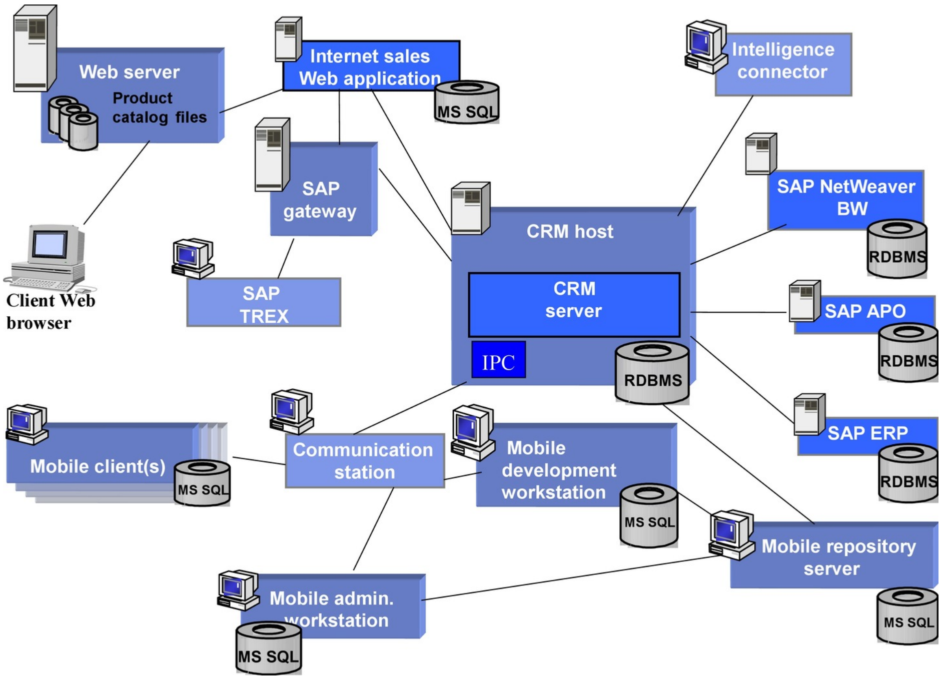


Figure 1: Technical System Landscape for SAP CRM

From a security point of view, the chosen system landscape leads to specific security-related issues that must be addressed during setup and configuration.

Recommendation

Perform a detailed security analysis and evaluation for a new or modified system landscape with all its components.

You may want to use external resources (for example, your company's security team or an external service provider) for security-related consulting or to perform the security assessment.

For more information about the technical system landscape, see the resources listed in the following table:

Table 3

Topic	Guide/Tool	Quick Link on SAP Service Marketplace
Technical description for SAP CRM and the underlying technological components such as SAP NetWeaver	*Master Guide for SAP Customer Relationship Management*	service.sap.com/crm-inst
Technical configuration High availability	*Technical Infrastructure Guide for SAP NetWeaver*	service.sap.com/instguides
Security	General security information	service.sap.com/security

1.4 Security Aspects of Data, Data Flow and Processes

The data flow in SAP CRM varies depending on the scenario or process that is used. The data transfer from SAP CRM to other SAP systems, such as SAP ERP and SAP NetWeaver BW, and to mobile clients is carried out by using SAP CRM Middleware. SAP CRM Middleware is an integral part of the CRM server. For more information, see the CRM Server [page 301] section.

The following figure shows the data flow in sales order processing as an example for the data flow in SAP CRM:

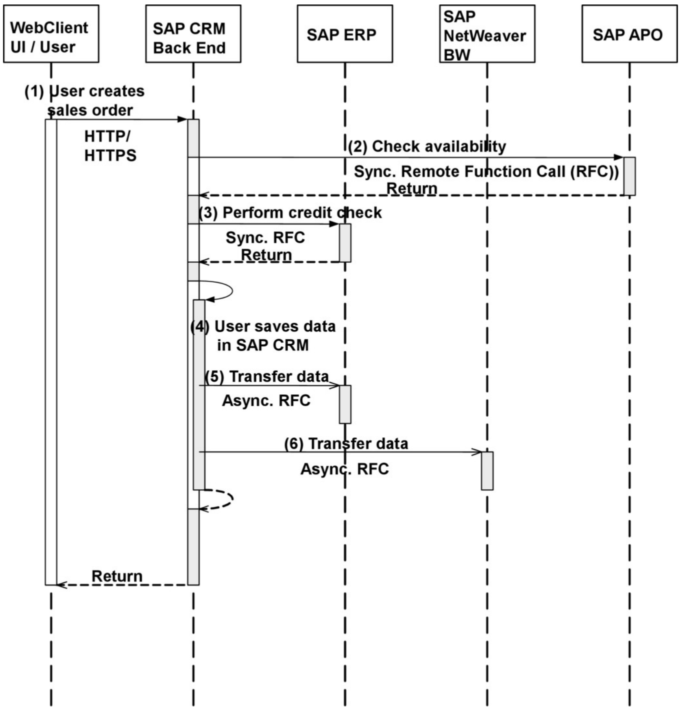


Figure 2: Overview of Process Steps for Sales Order Processing

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

Table 4

Step	Description	Security Measure
1	User creates sales order	• User type: Dialog user with assignment to business role and PFCG role • Communication protocol: HTTP or HTTPS
2	Perform availability check	Not applicable (synchronous RFC)
3	Perform credit check	Not applicable (synchronous RFC)
4	User saves data in SAP CRM	Not applicable
5	Transfer data to SAP ERP	• Not applicable (synchronous RFC) • If payment cards are used, see section Payment Card Security According to PCI-DSS [page 42].
6	Transfer data to SAP NetWeaver BW	Not applicable (synchronous RFC)

1.5 Security Dependency: SAP CRM and Other Components

SAP Customer Relationship Management (SAP CRM) is based on several other SAP components. The most important of these are:

- SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP), which is used, for example, for implementing the CRM server
- SAP NetWeaver Application Server Java (SAP NetWeaver AS Java), which is used to implement Java-based CRM components, such as SAP E-Commerce
- The SAP NetWeaver Business Warehouse (SAP NetWeaver BW) components, which are used for generating business intelligence reports

Each of the components has its own configuration options, which must be set correctly to provide an appropriate overall level of security. The tasks include not only configuration during normal operation but also activities to be performed before, during, and after installation (such as providing secure passwords during installation, changing default passwords after installation, or performing Customizing activities).

Note

It is not sufficient to set up and configure the functions of only those base components that are used for SAP CRM. All the available base component functions must be either configured correctly or disabled if not needed.

Recommendation

Read the appropriate configuration guides for each component. For more information, see Before You Start [page 8].

In addition, several external components at the network level, such as routers and firewalls, influence the overall security of the SAP CRM system landscape.

The following sections describe the security dependencies between the important SAP components and SAP CRM. Examples are used to illustrate why security in the underlying components is essential for the secure operation of SAP CRM.

SAP NetWeaver AS Security

SAP NetWeaver AS is the technical base for many SAP CRM components and, therefore, plays an important role in the security of SAP CRM. Since SAP CRM components run on top of SAP NetWeaver AS and also use its base functions to implement SAP CRM functions, any configuration weakness in SAP NetWeaver AS impacts SAP CRM directly.

Note

Since SAP NetWeaver AS integrates the ABAP and Java stacks, both stacks need proper configuration. For more information, see Application Server Java Security [page 13].

A central part of SAP CRM is the CRM server, which runs on the ABAP stack of SAP NetWeaver AS. The standard functions and interfaces of the ABAP stack must be configured appropriately to ensure secure operation of the CRM server component.

As part of its basic functions, SAP NetWeaver AS offers several interfaces to the network. This includes remote function call (RFC)-enabled function modules or services offered using the Internet Communication Framework (ICF).

Example

A standard function available from the ICF is the Simple Object Access Protocol (SOAP)-based RFC interface allowing RFC requests over HTTP. This interface is activated for use by another application. The SAP CRM scenario assumes that users access only the preceding SAP E-Commerce application. If the CRM server is not shielded properly by the firewall from HTTP access, any user can call any RFC functional module over HTTP.

For more information, see the *SAP NetWeaver Application Server ABAP Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP*.

1.5.1 Application Server Java Security

Application Server Java (AS Java) is, on the one hand, used to implement the SAP NetWeaver Application Server (SAP NetWeaver AS) Java stack, and on the other hand, available as a stand-alone component. It is a complete application server, offering a security environment based on user management and roles, as required by the J2EE specification. In addition, many services are offered to the network to conform to the J2EE specification. When using AS Java to run SAP Customer Relationship Management (SAP CRM) components – either as a Java stack within SAP NetWeaver AS or stand-alone – these default features must be configured securely. Secure configuration ensures secure operation of SAP CRM and prevents undesired side effects.

For more information, see the *SAP NetWeaver Application Server Java Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS Java*.

1.5.2 Firewalls and Perimeter Security

SAP Customer Relationship Management (SAP CRM) components are distributed over several computers and need to exchange data to provide their functions. This requires connection to a communication network. Without further restrictions, network communication is, in principle, possible between all components connected to the network. Since the data and functions require different levels of protection and access, firewalls – components that filter data packets sent over the network according to predefined filter rules – are used. Since the internal network must not be accessed by external users, firewalls are used to protect any access path crossing the border (or “perimeter”) between the external network and the company’s internal network. Access-restricting components such as dial-in routers with strong authentication mechanisms may also be used with firewalls for this purpose.

Although firewall and perimeter security are general topics, they affect security of any CRM installation directly.

Example

A CRM system uses a database to store data. For accessing the database, the CRM software uses a technical user account, which is configured to be the standard super administrator account with a default well-known password. No firewall exists to restrict communication with the CRM installation.

In this case, any user with access to the network and little technical knowledge can access the CRM database directly by using the well-known authentication information. The impact is more severe if such a network is accessible, without restrictions, from the Internet (for example, because of mobile users).

The security of CRM data is, therefore, also influenced by the network architecture and system landscape.

For more information, see Network and Communication Security [page 29].

For more information about network security in the context of SAP components, see SAP Service Marketplace at service.sap.com/securityguide.

1.6 Security of SAP CRM: Usage Scenario Examples

The following sections provide several typical usage scenarios for a sample SAP Customer Relationship Management (SAP CRM) key capability and demonstrate specific security issues that can occur.

From a security point of view, any usage scenario first requires a thorough assessment of the protection requirements. Following that, a security policy must be defined and appropriate safeguards must be implemented. Certain threats for IT systems depend on specific properties of a usage scenario; in such cases, special safeguards must be implemented.

The examples in this section are based on users who typically access the SAP CRM system:

- Internal (nonmobile) users: Employees of your company with a strong contractual relationship
- Internal (mobile) users: Employees who access SAP CRM from outside the company's network
- External users: Users who have a close relationship (such as a partnership contract) with the company or users who do not have a close relationship (for example, those who buy goods using the Internet)
- Anonymous users: Must not be trusted (from a security point of view)

Note

The user types are associated with varying levels of trust.

The level of protection for your SAP CRM scenario must be decided based on a threat analysis and the risk that your company is prepared to take according to your risk management requirements.

Internal (Nonmobile) Users

The enterprise services key capability is a typical intranet usage scenario that organizations can perform with SAP CRM. The SAP CRM components are located in a local intranet subnet and client access is only by employees of the company. The following figure shows a typical system landscape for this scenario:

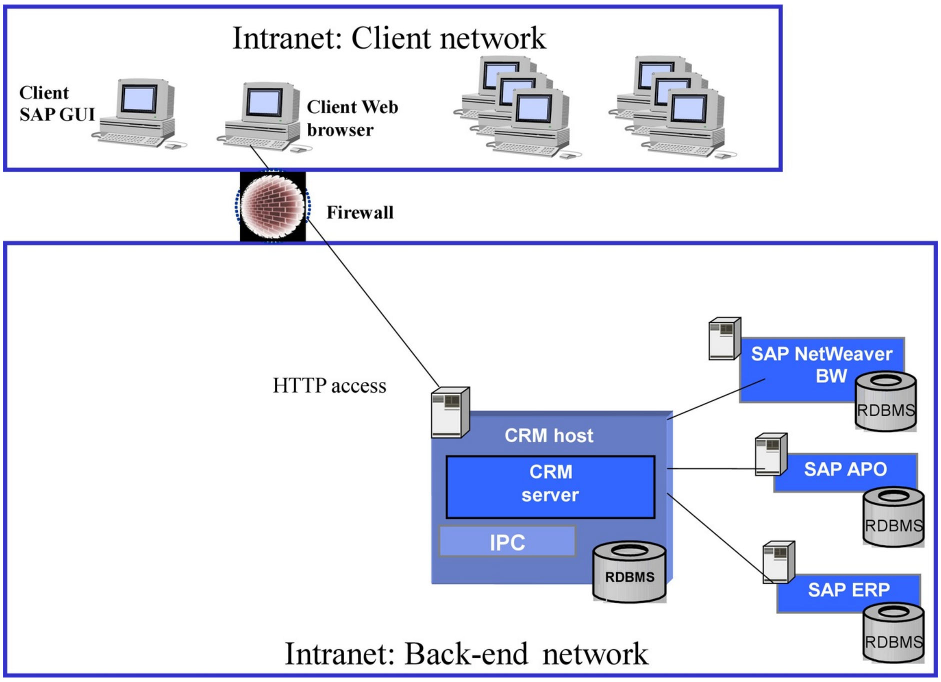


Figure 3: System Landscape for Scenario

The following intranet network segments are separated by a firewall or packet-filtering router:

- One segment contains the client machines of users.
- The other segment contains the server-side components.

Only internal users (employees) access SAP CRM components using the Web browser installed on their client machines, for example. The following security aspects are important:

- The firewall must shield the back-end system from all unwanted traffic (direct access to the CRM server or direct database access with Structured Query Language (SQL) client software). Therefore, correct configuration is necessary. The person performing the configuration must know the communication ports used by the various technical components.
- Correct access control settings to functions and data must be defined. The question of who is allowed to do what must be answered clearly.
- Data export must be prevented or made more difficult. This requires an assessment of the hardware (such as USB ports on client machines) and communication links (such as remote function call (RFC) destinations or database links).

For this scenario, the other security aspects – such as theft of client machines and threads from anonymous attackers on the Internet – are not relevant or do not play a dominant role.

Protection against internal attacks and against erroneous operation by inexperienced users is the prominent security task for this scenario. In any case, since this scenario involves employees with contracts, additional legal action can be taken in case of security violations.

Internal (Mobile) Users

The field sales key capability typically involves mobile users. For mobility reasons, special technical equipment and communication technologies must be used. In addition, mobile users need to operate while they are not connected to the CRM server and, therefore, the necessary data must be stored locally in the mobile device, such as a laptop computer.

The following figure shows a typical system landscape enabling mobile access to SAP CRM:

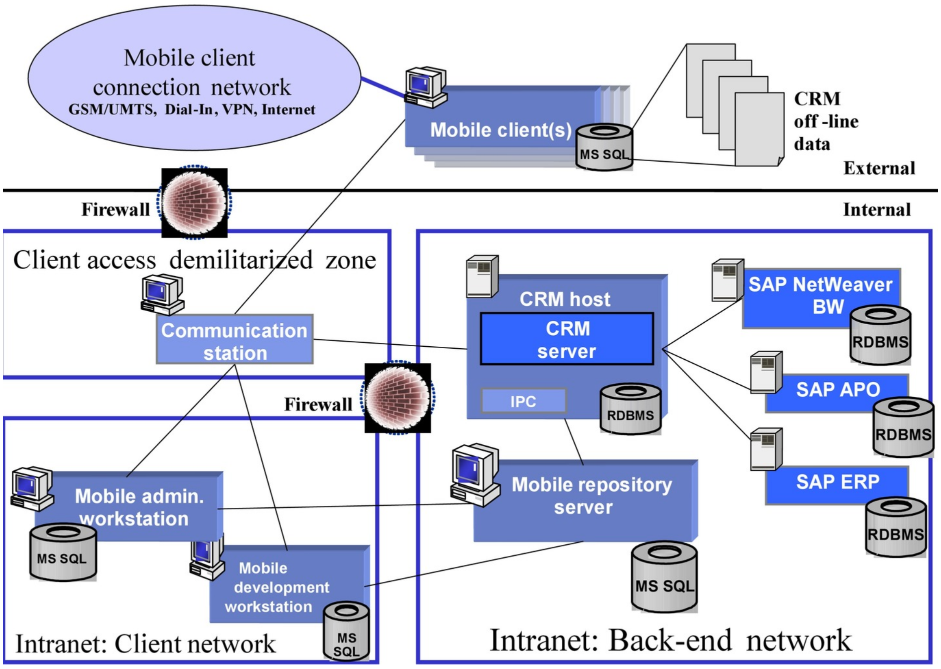


Figure 4: System Landscape for Mobile Access to SAP CRM

Besides the other components involved, SAP CRM uses the **communication station** as the communication hub for mobile clients. The connection can be realized with different communication technologies. The technologies used in this scenario result in specific security-related issues:

- User authentication is performed externally at the client machine and no back-end server is involved. Therefore, security of the client machine must be ensured.
- Security of the communication links between mobile client and the communication station must be ensured. Since SAP CRM data is synchronized using this communication link, any possibility of interfering with the communication link would compromise the quality of data transferred. This is especially important if untrusted networks are used.
- The mobile clients connect (with the company network) from external locations for synchronizing data with the CRM server. The access path must provide appropriate security (for both the client and the company network) to protect other resources in case the client machine has been compromised. Therefore, the communication station must be located in a secure and dedicated network and the communications relationships must be restricted by appropriate firewalls or filtering routers.
- SAP CRM data that is stored offline on the mobile clients must be protected to prevent access in the event of the machines being lost or stolen.
- The mobile client computer must be protected against viruses. This is necessary to prevent malware from accessing the local SAP CRM data or even the communication station during synchronization.
- Since the mobile client may be used in external networks (for example, customer networks or the Internet) or for other purposes than running the SAP CRM mobile application, hardening should be a best practice. This includes installing updates and patches, as well as reducing the number of software and services installed on the computer.

In addition to these prominent issues, correct access control configuration must be ensured at all levels: network, firewalls, machines, and SAP CRM components. In terms of complexity, the task of configuring and operating the system depends on the usage scenario and the additional components that are required.

Anonymous Users

Users who access the SAP CRM system without prior authentication could be part of almost any usage scenario. Public information for customers (such as news and FAQs) may be accessed this way. Customer forums (for example, developer networks) that the company provides to allow discussions among customers or between the customers and the company also involve anonymous users. In this scenario, adequate access control settings are essential for the repositories (for example, knowledge management repository) and the data that they contain; especially if public and nonpublic information is stored together: Flaws in the access control settings may give anonymous users access to nonpublic information.

> ➜ Recommendation
>
> From a security perspective, we recommend that you treat normal users the same as anonymous users; if your access control settings are not adequate, a normal user could compromise the security of data just like any anonymous user could.

1.7 Business Roles

In SAP Customer Relationship Management (SAP CRM), you can define business roles so that they can do the following:

- Assign function profiles, including the navigation bar profile
- Deactivate work centers
- Make work-center group links visible in the menu and in work center pages
- Make direct group links visible in the menu
- Assign an appropriate authorization role using the profile generator (transaction `PFCG`)

SAP CRM comes with a set of pre-defined business roles. For information about using a pre-defined role or copying an existing role and adjusting it to your needs, see Customizing for *Customer Relationship Management* under *UI Framework* > *Business Roles* > *Overview*.

If you want to create a business role from scratch, use the following activities in Customizing for *Customer Relationship Management*:

Table 5

Setting	Path to Customizing Activity
Configuration key	*UI Framework* > *UI Framework Definition* > *Define Role Configuration Key*
Authorization role	*UI Framework* > *Technical Role Definition* > *Define Authorization Role*
Business role	*UI Framework* > *Business Roles* > *Define Business Role*
Organizational assignment	*UI Framework* > *Business Roles* > *Define Organizational Assignment*
Logical links, work-center link groups, direct link groups, and navigation bar profiles	*UI Framework* > *Technical Role Definition* > *Define Navigation Bar Profile*

1.8 User Administration and Authentication

SAP Customer Relationship Management (SAP CRM) uses the user management and authentication mechanisms provided by SAP NetWeaver, in particular the SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP and Java technology. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide* and the *SAP NetWeaver Application Server Java Security Guide* also apply to SAP CRM.

You can access these guides in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server*.

SAP CRM uses the following authentication mechanisms:

- Standard SAP NetWeaver authentication against the ABAP stack, for users directly accessing the SAP CRM components based on ABAP. For more information about authentication when using the Web UI, see UI Framework [page 310].
- Standard SAP NetWeaver platform authentication against the Java stack (AS Java), for users directly accessing the SAP CRM components based on Java.
- Standard Windows authentication and mobile client authentication for mobile users in SAP CRM.

> **Note**
>
> Except for the mobile user scenarios, after the first authentication, single sign-on (SSO) in SAP NetWeaver is used to transparently authenticate users to other components that they access directly.

The following sections contain user administration and authentication information that specifically applies to SAP CRM:

- User Management [page 18]

  This section lists the tools for user management, the types of users required, and the standard users that are delivered with SAP CRM.
- User Data Synchronization [page 24]

  SAP CRM shares user data with different systems (depending on the usage scenarios). This section describes how user data is synchronized with other systems. It also describes which user data information must be managed in different systems.
- Integration with the Single Sign-On Environment [page 24]

  This section describes how SAP CRM supports SSO mechanisms.

> **Note**
>
> The individual sections for component-specific guidelines contain information about special considerations for specific key capabilities.

1.8.1 User Management

SAP Customer Relationship Management (SAP CRM) uses the mechanisms of SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP and Java, such as tools, user types, and password policies, and so on, for user management. In scenarios where other components such as mobile clients are involved, additional user management mechanisms and tools must be used.

User Management Tools

Though profile and role management is related to authorization management, it is included in this section because it also involves user accounts. The following table contains a list of the tools for user management and user administration with SAP CRM:

Table 6

Tool	Description	Relevant SAP CRM Scenario
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (transaction `SU01`) and profile generator (transaction `PFCG`) If user administration is performed centrally, the administration tool is the Central User Administration. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security* › *Identity Management* › *User and Role Administration of Application Server ABAP*.	For any regular SAP CRM user, a user master record must exist. This user account is required to perform access control based on profiles and roles. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security* › *Identity Management* › *User and Role Administration of Application Server ABAP* › *Administration of Users and Roles*. Note Additional actions must be performed in the access control engine (ACE) before a user is deleted. For more information, see Component-Specific Guidelines: Partner Channel Management [page 282] and Access Control Engine [page 324]. In addition to normal users, technical users must be created and maintained in the ABAP stack for some SAP CRM components. For more information, see Interactive Product Configuration User Interface [page 275].	All SAP CRM scenarios
Business partner maintenance with SAP NetWeaver AS ABAP: Transaction *Maintain Business Partner* (`BP`)	For more information, see Component-Specific Guidelines: Web Channel Enablement [page 241].	Web Channel enablement – SAP E-Commerce for SAP CRM
User management with SAP NetWeaver AS Java: User management engine (UME) For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant*	Access to administration pages, which are part of several SAP CRM applications, is controlled using AS Java security. The appropriate AS Java users must be created and maintained. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ›	Web Channel enablement – E-service – Internet customer self service Web Channel enablement – SAP E-Commerce CRM powered by SAP NetWeaver – SAP Internet Pricing and Configurator (IPC)

Tool	Description	Relevant SAP CRM Scenario
release> ▸ *Application Help* ▸ *Function-Oriented View* ▸ *Security* ▸ *Identity Management* ▸ *User Management of the Application Server Java* .	*Security* ▸ *Identity Management* ▸ *User Management of the Application Server Java* ▸ *Administration of Users and Roles* . In some cases, the administrator user account of the AS Java must be used to access the administration pages. For more information, see Component-Specific Guidelines: Web Channel Enablement [page 241] and Interactive Product Configuration User Interface [page 275].	
Web-based user management	Used for business-to-business users only. For more information, see Component-Specific Guidelines: Web Channel Enablement [page 241].	Web Channel enablement – SAP E-Commerce for SAP CRM
User and user group maintenance with SAP NetWeaver AS ABAP in Customizing for *Customer Relationship Management* under *Basic Functions* ▸ *Access Control Engine*	The ACE is used to perform access control within SAP CRM scenarios. Permissions are granted based on user groups. Group management involves assigning users created using the *User Maintenance* transaction to ACE user groups. Note Additional actions must be performed in the ACE before a user created using the *User Maintenance* transaction is deleted. For more information, see Component-Specific Guidelines: Partner Channel Management [page 282] and Access Control Engine [page 324].	Partner channel management
Mobile client administration console in the CRM server	For each mobile user, a user account must be created. This account is used to log on to the mobile application in the mobile device (such as a laptop). For more information, see Component-Specific Guidelines: Field Applications [page 223].	Field applications: Mobile sales and mobile service
Structured Query Language (SQL) database administration client	The database that is used to store SAP CRM data on the mobile device is accessed using a technical account. Note The default password of the technical account must be changed after installation. For more information, see Component-Specific Guidelines: Field Applications [page 223].	Field applications: Mobile sales and mobile service

Tool	Description	Relevant SAP CRM Scenario
Windows user management	For each mobile client user, a Windows user account must be generated. This account is used to log on to the Windows operating system. Depending on the Windows setup (stand-alone versus domain) local or domain users must be created. Appropriate user accounts must exist on the client machines and the communication station. For more information, see Component-Specific Guidelines: Field Applications [page 223] and Mobile Client Synchronization [page 233].	Field applications: Mobile sales and mobile service

User Types

It can be necessary to specify different security policies for different types of users. For example, your policy may specify that users who perform tasks interactively must change their passwords regularly, whereas users who run jobs in the background need not do so.

The user types that are required for SAP CRM include all SAP user types. The following table provides an overview of the user types:

Table 7

User Type		Description
Individual users	Dialog user created using the *User Maintenance* transaction	Normal SAP CRM users who access the SAP CRM functions. Different access paths are possible requiring other user types for authentication. All such users are mapped to the user created in the *User Maintenance* transaction (for example, using single sign-on).
	Internet user	May be required for specific scenarios. The same policies apply as for dialog users.
	AS Java user	For authenticating access to administrative pages of certain SAP CRM components running on the AS Java.
	Application-level user	For authenticating access to mobile clients. These users must be created using the administration console on the CRM server.
Technical users	Service user	For running services.
	Communication user	For authenticating communication connections, providing access restrictions, and limiting authorization for access requests using communication connections.
	Background user	For background processing, such as executing workflow processes.

For more information about security features in SAP NetWeaver, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *User Administration and Authentication*.

The following table gives an overview of the user types required in the SAP CRM key capabilities:

Table 8

Key Capability	User Types	Description
Sales Service	- Dialog user created using the *User Maintenance* transaction - Background user created using the *User Maintenance* transaction	Individual users to be able to use the delivered standard processes. For more information, see business roles SALESPRO and SERVICEPRO in the Authorizations [page 25] section. Initial identification parameters, such as passwords and certificates for these users, are not provided by SAP.
Marketing — Product proposals	- User created using the *User Maintenance* transaction - Internet user	If product proposals are used in SAP E-Commerce, besides users, Internet users are also required. Product association rules for cross-selling, up-selling, and down-selling and products for top n lists can be determined in a business information system and uploaded to SAP CRM. This action requires a remote function call (RFC) connection with a user and password.
Marketing - External list management	- Dialog user created using the *User Maintenance* transaction - Workflow user created using the *User Maintenance* transaction	The dialog user creates and maintains external lists. This action includes activities such as: - Creating an external list - Marking process steps that must be executed in the workflow - Deleting an external list The workflow user executes the marked process steps in external list management in the background through a workflow. Both are standard users created using the *User Maintenance* transaction.
Field applications - Mobile sales - Mobile service	Application-level user	The customer must create these users by using the administration console on the CRM server. According to the defined subscription, only those users that are created for the site mobile clients are replicated to all mobile clients. The system administrator at the customer's site creates individual interactive users.
Field applications - Mobile client synchronization	- Windows domain user to connect the mobile client to the communication station - SAP ERP user to connect the communication station to the CRM server - A technical user for each destination on the communication station	N/A

Key Capability	User Types	Description
Web channel – E-service	• Dialog users created using the *User Maintenance* transaction and service users • AS Java administrator for access to administrative pages	N/A
Web channel – E-commerce	• Dialog users created using the *User Maintenance* transaction and service users • AS Java users • AS Java administrator	User types depend on the usage scenario.
Interaction center – Interaction center WebClient	• Dialog users created using the *User Maintenance* transaction • Service users • Communication users created using the *User Maintenance* transaction	These users are needed for the following purposes: • System user ○ RFC user to connect to back-end ERP system (optional, but recommended) Note The advantage is that, because this user is for RFC use only, the user has no system dialog access. Therefore, individuals cannot inadvertently access the system and cause damage. ○ Java Connector (JCo) user to communicate between AS Java and ABAP (Java configuration only) • Individual user in the standard WebClient UI who can access all the functions in the interaction center WebClient (IC WebClient) scenarios For more information, see business role `IC_AGENT` in the Authorizations [page 25] section.
Interaction center - E-mail response management system	User created using the *User Maintenance* transaction	N/A
Interaction center - Interaction center manager	User created using the *User Maintenance* transaction	N/A
Partner channel management - Channel sales management for high tech and partner channel management - Contracts and	User created using the *User Maintenance* transaction	N/A

Key Capability	User Types	Description
chargeback for pharmaceutical		

Standard Users

The different SAP key capabilities use different standard users.

1.8.2 User Data Synchronization

User data synchronization (that is, synchronization of user accounts and the associated information, such as passwords) is based on the standard SAP user management synchronization mechanisms. Therefore, the standard recommendations for the SAP NetWeaver Application Server (SAP NetWeaver AS) apply to SAP Customer Relationship Management (SAP CRM) also.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *User Administration and Authentication*.

Note

If multiple CRM servers are required or if a central user management must be used, central user administration (CUA) is involved.

For all field applications, user accounts must be available for authenticating access to the mobile applications. This requires manual application-level actions for creating and distributing the user account information (in particular, the user name and password).

1.8.3 Integration with the Single Sign-On Environment

Most SAP Customer Relationship Management (SAP CRM) components are based on standard SAP components and, therefore, support the single sign-on (SSO) mechanisms provided by SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP and Java. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server Security Guide* apply to SAP CRM also.

Note

In SAP CRM scenarios involving multiple components, the relevant components (such as the CRM server) must be configured for SSO to prevent the need for component-specific authentication.

For SAP CRM, SSO is available for all scenarios. The only exception is field applications, where users work offline and use mobile devices. In this case, users must be authenticated when they log on to Windows and then when they start the mobile application.

Secure Network Communication

Secure network communication (SNC) is available for user authentication and provides an SSO environment when using remote function call (RFC).

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *Protecting Your Productive System (Change & Transport System)* > *Security for the RFC Connections*.

SAP Logon Tickets

SAP CRM 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. Thereafter, users can access the systems directly.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *User Administration and Authentication* > *Integration in Single Sign-On Environments* > *Logon Tickets*.

Client Certificates

As an alternative to user authentication using user IDs and passwords, users who use a Web browser as the front-end client can also provide X.509 client certificates for authentication. In this case, user authentication is performed on the Web server using the secure sockets layer (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, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *User Administration and Authentication* > *Integration in Single Sign-On Environments* > *Logon Tickets* > *Client Certificates*.

> Note
>
> Using client certificates does not automatically provide SSO; this is only an alternative method of authentication. Nevertheless, SSO based on SAP logon tickets can be used together with this kind of user authentication.

SSO is not available for field applications; Windows authentication is used for system access and for authentication at a technical level during data synchronization; user name and password authentication is used for accessing the mobile applications.

1.9 Authorizations

SAP Customer Relationship Management (SAP CRM) uses the authorization provided by SAP NetWeaver Application Server (SAP NetWeaver AS). Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server Security Guide* apply to SAP CRM.

For more information, see *AS ABAP Authorization Concept* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for the Application Server* › *Security Guides for the AS ABAP* › *SAP NetWeaver Application Server ABAP Security Guide*.

The SAP NetWeaver AS authorization concept is based on assigning authorizations to users depending on roles. For role administration, use the profile generator (transaction `PFCG`) for SAP NetWeaver AS ABAP and the user management engine's user administration console for SAP NetWeaver AS Java.

In addition to these standard authorization mechanisms, SAP CRM uses the following mechanisms for authorization within SAP CRM scenarios:

- Authorization roles are assigned to business roles. For more information, see Business Roles [page 17].
- The access control engine (ACE) is used to configure access to CRM data in the CRM server. Activation and configuration of ACE is done in Customizing in the system.
- For all scenarios involving mobile clients that store replicated CRM data, additional SAP CRM application-specific authorizations must be configured and maintained. These authorizations determine the data that must be replicated and synchronized with a mobile client. The *Administration Console* (`SMOEAC`) transaction in SAP CRM is used to perform this configuration.

Note

All the authorization mechanisms must be configured (and configured consistently) to provide appropriate security.

Recommendation

Since there is no general authorization configuration that fits all possible use scenarios, we recommend that you design an authorization concept tailored to your specific use scenario.

Standard Roles

The different SAP key capabilities use different roles. For more information, see the component-specific sections. The following is an overview of standard roles delivered by SAP and the corresponding PFCG roles:

Table 9

Business Role	PFCG Role	Description
AIC_MANAGER	SAP_CRM_UIU_AIC_MANAGER	AIC Manager
ANALYTICSPRO	SAP_CRM_UIU_ANALTYICSPRO	Analytics Professional
AUT-PM	SAP_CRM_UIU_AUT_PARTNERMANAGER	Automotive Partner Manager
AXT	SAP_AXT_EXTENSIBILITY_ADMIN	Application Enhancement Tool
CASEWORKER	SAP_CRM_UIU_CASEWORKER	Case Worker (Social Services)
CHM-CM	SAP_CRM_UIU_CHM_CHANNELMANAGER	Channel Manager
CHM-PM	SAP_CRM_UIU_CHM_PARTNERMANAGER	Partner Manager

Business Role	PFCG Role	Description
CRMGRMPRGMAN	SAP_CRM_UIU_GRANTOR_PROG_MNGR	Grantor Program Manager
DETECTIVE	SAP_CRM_UIU_ICM_PROFESSIONAL	Detective
ECO-MANAGER	SAP_CRM_UIU_ECO_MANAGER	Web Channel Manager
ETC_IC	SAP_CRM_UIU_ETC_IC_AGENT	Toll Collection IC Agent
EWA_IC_AGENT	SAP_CRM_UIU_EWA_IC_AGENT	Waste & Recycling IC Agent
FCC	SAP_CRM_UIU_FCC_AGENT	Financial IC Agent
FCC_FSCD	SAP_CRM_UIU_FSCD_FCC_AGENT	Financial IC Agent Insurance
FCC_LEAS	SAP_CRM_UIU_FS_FCC_AGENT	Financial IC Agent Leasing
FCC_PC_ERP	SAP_CRM_UIU_FCC_PC_ERP_AGENT	Financial IC Agent — Prov Ctr in ERP
FCC_PSCD	SAP_CRM_UIU_PSCD_FCC_AGENT	Financial IC Agent PS
FSAO_MANAGER	SAP_CRM_UIU_FSAO_MANAGER	FS Sales Manager
HT-CHM-CM	SAP_CRM_UIU_HT_CHM_CHANNEL_MAN	High Tech Channel Manager
HT-CHM-PM	SAP_CRM_UIU_HT_CHM_PARTNER_MAN	High Tech Partner Manager
IC_AGENT	SAP_CRM_UIU_IC_AGENT	InteractionCenter Agent
IC_AGENT_ECS	SAP_CRM_UIU_IC_AGENT	Interaction Center Agent ECS
IC_AIC_AGENT	SAP_CRM_UIU_IC_AIC_AGENT	Accounting IC Agent
IC_AUTO	SAP_CRM_UIU_AUTO_IC_AGENT	InteractionCenter Agent Auto
IC_EIC_AGENT	SAP_CRM_UIU_IC_AGENT_EIC	Employee Service Center Agent
IC_ITSDAGENT	SAP_CRM_UIU_IC_ITSDAGENT	IT Service Desk Agent
IC_LOY_AGENT	SAP_CRM_UIU_LOY_IC_AGENT	Loyalty Prof IC Agent
IC_MANAGER	SAP_CRM_UIU_IC_MANAGER	IC Manager
IC_SSC_AGENT	SAP_CRM_UIU_IC_AGENT_SSC	Shared Service Center Agent
IC_TIC_AGENT	SAP_CRM_UIU_TIC_AGENT	Travel IC Agent
IPMRIGHTSMAN	SAP_CRM_UIU_IPM_RIGHTSMANAGER	Rights Manager
ITSERVICEPRO	SAP_CRM_UIU_SRQM_PROFESSIONAL	IT Service Professional

Business Role	PFCG Role	Description
ITSERVREQU	SAP_CRM_UIU_SRQM_REQUESTER	IT Service Requester
LEASING	SAP_CRM_UIU_LAM_MANAGER	Leasing Manager
LOY_PRO	SAP_CRM_UIU_LOY_PROFESSIONAL	Loyalty Professional
MARKETINGPRO	SAP_CRM_UIU_MKT_PROFESSIONAL	Marketing Professional
MEDIA_IC	SAP_CRM_UIU_MEDIA_IC_AGENT	Interaction Center Agent
PHA-CLM	SAP_CRM_UIU_PHA_CLM	Life Sciences/Pharma CLM
PROFSERVICES	SAP_CRM_UIU_PRS_PROFESSIONAL	Professional Services
PROVIDER_DL	SAP_CRM_UIU_PROVIDER_DL_AGENT	Provider Dealer
PROVIDER_IC	SAP_CRM_UIU_PROVIDER_IC_AGENT	Provider IC Agent
SALESPRO	SAP_CRM_UIU_SLS_PROFESSIONAL	Sales Professional
SERVICEPRO	SAP_CRM_UIU_SRV_PROFESSIONAL	Service Professional
SPL	SAP_CRM_UIU_SPL_PROFESSIONAL	Service Parts Management
SSF_OCCUSER	SAP_CRM_UIU_SSF_OCCUSER	SSF Occasional User Role
TEL-CM	SAP_CRM_UIU_TEL_CHANNELMANAGER	Telco Channel Manager
TEL-PM	SAP_CRM_UIU_TEL_PARTNERMANAGER	Telco Partner Manager
TELCO_FCC	SAP_CRM_UIU_TELCO_FCC_AGENT	Telco: Financial IC Agent
TPM_PRO	SAP_CRM_UIU_TPM_PROFESSIONAL	TPM Professional
TRD_CLM_PRO	SAP_CRM_UIU_TCM_PROFESSIONAL	Trade Claims Professional
TRD_FIN_PRO	SAP_CRM_UIU_TFM_PROFESSIONAL	Trade Finance Professional
UIF	SAP_BC_SRV_PPF_ADMIN	UI Framework Test Role
UTIL_IC	SAP_CRM_UIU_UTIL_IC_AGENT	Utilities IC Agent

Business Role	PFCG Role	Description
`UTIL_IC_LEAN`	`SAP_CRM_UIU_UTIL_IC_LEAN_AGENT`	Utilities IC Agent (Lean)
`UTIL_IC_REG`	`SAP_CRM_UIU_UTIL_IC_REG_AGENT`	Utilities IC Agent (Regulated)
`UTIL_SALES`	`SAP_CRM_UIU_SALES_UTILITES`	Utilities Sales for KAM

Standard Authorization Objects

The different SAP key capabilities use different authorization objects. For more information, see the component-specific sections.

1.10 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 SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *Function-Oriented View*: Search for *Activating HTTP Security Session Management on AS ABAP*.

Session Security Protection on the AS Java

Using the visual administrator, on the AS Java, set the properties described in *Session Security Protection* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS Java* > *SAP NetWeaver Application Server Java Security Guide* > *Other Security Relevant Information*.

1.11 Network and Communication Security

The network infrastructure plays an important role in protecting your system. Your network needs to support the communication that is required for your business without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and the 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 back-end system's database and files. Additionally, if users are unable to connect to the server local area network (LAN), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP Customer Relationship Management (SAP CRM) is based on the topology used by SAP NetWeaver. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* apply to SAP CRM also. Specifics for SAP CRM are described in the following paragraphs:

- *Communication Channel Security*

  This paragraph describes the communication paths and protocols used by SAP CRM.
- *Network Security*

  This paragraph describes the recommended network topology for SAP CRM. 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 CRM.
- *Communication Destinations*

  This paragraph describes the information needed for the various communication paths, such as which users are used for which communications.

For more information, see the following sections in the *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* ◀:

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability Technologies*

Communication Channel Security

The following table lists the general communication paths used by SAP CRM, the protocol used for the connection, and the type of data transferred:

Table 10

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	N/A	Passwords, all sensitive CRM data such as credit card information, customer data, conditions, and so on
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, conditions, and so on
CRM server to CRM server	Remote function call (RFC)	System ID, client, host name, and all application data	System information and CRM data
CRM server to ERP server	RFC	System ID, client, host name, and all application data	System information and CRM data
CRM server to business intelligence (BI) server	RFC	System ID, client, host name, and all application data	System information and CRM data
Mobile client to communication station	Distributed Component Object Model (DCOM)	Windows authentication, mobile client ID data, and all application data	User information, system information, and sensitive CRM data

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
	(Windows Remote Procedure Call (RPC))		
Communication station to CRM server	RFC	System ID, client, host name, and all application data	User information, system information, and sensitive CRM data

DIAG and RFC connections can be protected using secure network communication (SNC). HTTP connections are protected using the secure sockets layer (SSL) protocol.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *Network Security for SAP NetWeaver AS ABAP*.

Recommendation

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

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Network and Communication Security* > *Transport Layer Security*.

Virus Scan Profiles

Attackers can abuse a file upload to modify displayed application content or to obtain authentication information from a legitimate user. Usually, virus scanners are not able to detect files designed for this kind of attack. For this reason, the standard SAP virus scan interface includes options to protect the user and the SAP system from potential attacks.

For more information about the behavior of the virus scanner when default virus scan profiles are activated, see SAP Note 1693981 (*Unauthorized modification of displayed content*).

For information about the interaction center virus scan profile `/IC_CCS_MCM/ICI_MAIL` that enables the scanning of e-mails that enter the system through the Integrated Communication Interface, see the E-Mail Response Management System [page 213] section.

Network Security

Network security is important for the overall security of an SAP CRM system landscape. The Technical System Landscape [page 9] section describes the system landscape and the SAP CRM components that are necessary depending on the application scenario and key capability to be used.

Different components of SAP CRM can be operated in different network segments. Certain components, however, must be accessible by the users or customers directly (for example, using HTTP or HTTPS protocol). Consequently, such components must be located in the demilitarized zone (DMZ) and, therefore, are more prone to attacks. Appropriate hardening and network access restrictions are necessary. In scenarios where Internet access is necessary, you may not want to use the same components for storing internal CRM information.

Note

For more information about the system landscape, see the *SAP Customer Relationship Management Master Guide* on SAP Service Marketplace at service.sap.com/crm-inst > *<Choose release>* > *Plan*.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose release>* > *Security Information* > *Security Guide* > *Network and Communication Security*.

SAP CRM runs on SAP NetWeaver and uses the ports from the AS ABAP or AS Java.

Note

For more information about AS ABAP Ports, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *Network Security for SAP NetWeaver AS ABAP* > *AS ABAP Ports*.

For more information about AS Java Ports, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS Java* > *SAP NetWeaver Application Server Java Security Guide* > *Network Security* > *AS Java Ports*.

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, also see *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Developer Network at sdn.sap.com/irj/sdn/security > *Infrastructure Security* > *Network and Communications Security*.

In addition to the SAP NetWeaver ports, field applications involve mobile clients and the corresponding infrastructure (such as the communication station), which are based on Windows, using other communication ports.

Note

For more information about the specific ports used by SAP CRM components in the mobile scenarios, see Mobile Client Synchronization [page 233].

Communication ports must be accessible only to the components that use the ports for communication. Firewalls, packet filters, or operating system functions for port filtering can help to shield communication ports from unwanted traffic.

All SAP CRM systems must be protected by a firewall that restricts the communication relationships.

Recommendation

Use a firewall between SAP CRM clients (such as Web browsers) and the servers. This firewall must be configured to allow only client access to the communication ports at the allowed server systems. All other communication attempts must be prevented.

For specific usage scenarios, you must consider additional firewalls, packet filters, or even application-level firewalls (such as HTTP proxies with URL filters), depending on the required protection level for the data stored in SAP CRM.

Note

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Network and Communication Security* > *Using Firewall Systems for Access Control*.

Note

There is no typical network layout for SAP CRM; the layout depends on the key capability that is used.

Communication Destinations

The different SAP key capabilities use different communication destinations. For more information, see the component-specific sections.

For general security information in RFC scenarios, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for Connectivity and Interoperability Technologies* > *RFC/ICF Security Guide*.

1.12 Data Synchronization

Synchronizing Customer Relationship Management (CRM) data appropriately between all SAP CRM components is an important task and requires appropriate security. SAP CRM uses middleware for all data synchronization tasks. Middleware in SAP CRM takes care of the technical processes involved in data synchronization and allows configuration of distribution restrictions. This helps you control the information that is available in different SAP CRM components.

Middleware in SAP CRM is used to distribute and synchronize CRM data between:

- Different SAP CRM systems
- SAP CRM and mobile clients
- SAP NetWeaver Business Warehouse (SAP Net Weaver BW) and SAP CRM
- SAP ERP and SAP CRM

Note

Middleware in SAP CRM must be configured in Customizing for *Customer Relationship Management* under *CRM Middleware and Related Components*.

For more information about middleware in SAP CRM, see Mobile Client Synchronization [page 233].

1.13 Data Storage Security

SAP Customer Relationship Management (SAP CRM) stores CRM data in the following locations:

- Locations that you have configured (for example, by using middleware in SAP CRM to replicate data to mobile clients)
- Locations that result from properties of the technical components used for realizing SAP CRM (such as data in log files or message queues at components used for communication path realization)

Related Security Guides

Table 11

Application	Guide	Most Relevant Sections or Specific Restrictions
SAP NetWeaver	Security guide	*Database Access Protection* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for the Operating System and Database Platforms*
SAP NetWeaver Application Server (SAP NetWeaver AS)	Security guide	*Secure Store & Forward Mechanisms (SSF) and Digital Signatures* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* .

The following locations must be considered for storing data securely:

- The CRM server stores all CRM data in its database. Therefore, the database must be secured appropriately. In addition, credit card information must not be stored in clear text form in the database. A scrambling mechanism must be used to protect the information.

  Note

  Storing credit card information in protected form requires installation and activation of additional software (cryptographic software provided by SAP).

  Recommendation

  Use additional protection mechanisms for credit card information.

  For more information about security aspects for credit card processing, see section Payment Card Security According to PCI-DSS [page 42].

  For more information about database security, see *Database Access Protection* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for the Operating System and Database Platforms* .

- For scenarios involving mobile clients, the following must be considered:
  - Each mobile client stores all CRM data in a local database. Therefore, protection against the risk of theft of the mobile devices is essential.

    Recommendation

    Use hard disk encryption for mobile clients to protect all data, including CRM data. For more information about data security on mobile clients, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guide for SAP NetWeaver Mobile* .

  - To synchronize mobile clients with the CRM server, several intermediate components are used. These components handle all the CRM data during the synchronization process and also store all or parts of the information locally (for example, in local queues or log files). To provide appropriate protection for CRM data, all these components must be configured securely at all levels. This also includes minimal file system permissions and system hardening.

- In scenarios involving Web browser access (that is, through clients running a Web browser), the information that is retrieved by the client is stored in the Web browser's cache. These scenarios require adequate security measures.

➡ Recommendation

Instruct users and customers to clear their Web browser cache after accessing SAP CRM information. If manual deletion is not feasible, a script can be used to clear the cache automatically when the user logs off.

Important SAP Notes

Use the following two SAP Notes to obtain a license for the SAP cryptographic software:

Table 12

SAP Note	Short Text	Comment
597059	License conditions of SAP Cryptographic Library	The SAP cryptographic software is required in various components to encrypt or decrypt data for storage and communication.
397175	SAP Cryptographic Software - Export control	N/A

i Note

Check regularly for SAP Notes on the security of the application.

1.14 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

i Note

In the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

Table 13: Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.
Deletion	Deletion of **personal data** so that the data is no longer usable.
Retention period	The time period during which data must be available.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization.

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- **Access control**: authentication features as described in section User Administration and Authentication [page 18]
- **Authorizations**: authorization concept as described in section Authorizations [page 25]
- **Read access logging**: as described in section Read Access Logging [page 39]
- **Communication Security**: as described in the sections Network and Communication Security [page 29] and Security Aspects of Data, Data Flow and Processes [page 10]
- **Availability control**: as described in:
  - Section Data Storage Security [page 33]
  - *Administration of Databases* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com
  - SAP business continuity documentation in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *Function-Oriented View* > *Solution Life Cycle Management* > *SAP Business Continuity*
- **Separation by purpose**: is subject to the organizational model implemented and must be applied as part of the authorization concept

> ⚠ Caution
>
> The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Configuration of Data Protection Functions

Certain central functions that support data protection compliance are grouped in Customizing for *Cross-Application Components* under *Data Protection*.

Additional industry-specific, scenario-specific or application-specific configuration might be required. For information about the application-specific configuration, see the application-specific Customizing in the transaction `SPRO`.

1.14.1 Deletion of Personal Data

SAP CRM might process data (personal data) that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544.

The SAP Information Lifecycle Management (ILM) component supports the entire software lifecycle including the storage, retention, blocking, and deletion of data. SAP CRM uses SAP ILM to support the deletion of personal data as described in the following sections.

SAP delivers an end-of-purpose check for SAP CRM.

All applications register an end-of-purpose check (EoP) in the Customizing settings for the blocking and deletion of the business partner. For information about the Customizing of blocking and deletion for SAP CRM, see *Configuration: Simplified Blocking and Deletion*.

End of Purpose Check (EoP)

An end of purpose check determines whether data is still relevant for business activities based on the residence period defined for the data. The retention period of data consists of the following phases.

- **Phase one**: The relevant data is actively used.
- **Phase two**: The relevant data is actively available in the system.
- **Phase three**: The relevant data needs to be retained for other reasons.

  For example, processing of data is no longer required for the primary business purpose, but to comply with legal rules for retention, the data must still be available. In phase three, the relevant data is blocked. Blocking of data prevents the business users of SAP applications from displaying and using data that may include personal data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

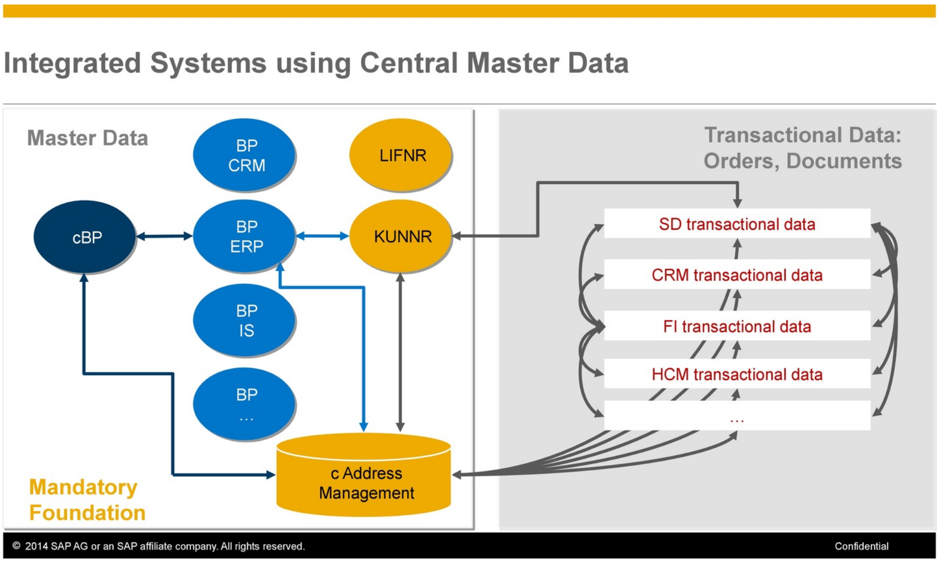
- **Display**: The system does not display blocked data.
- **Change**: It is not possible to change a business object that contains blocked data
- **Create**: It is not possible to create a business object that contains blocked data.
- **Copy/Follow-Up**: It is not possible to copy a business object or perform follow-up activities for a business object that contains blocked data.
- **Search**: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.

It is possible to display blocked data if a user has special authorization; however, it is still not possible to create, change, copy, or perform follow-up activities on blocked data.

For information about the configuration settings required to enable this three-phase based end of purpose check, see *Process Flow* and *Configuration: Simplified Blocking and Deletion*.

Integration with Other Solutions

In the majority of cases, different installed applications run interdependently as shown in the following graphic.



Integrated Systems using Central Master Data

Master Data

BP CRM

LIFNR

cBP

BP ERP

KUNNR

BP IS

BP ...

c Address Management

Mandatory Foundation

Transactional Data: Orders, Documents

SD transactional data

CRM transactional data

FI transactional data

HCM transactional data

...

© 2014 SAP AG or an SAP affiliate company. All rights reserved.

Confidential

Figure 5

An example of an application that uses central master data is an SAP for Healthcare (IS-H) application that uses the purchase order data stored in Financial Accounting (FI) or Controlling (CO).

The following are examples of typical integration scenarios for SAP CRM:

- Integration of SAP CRM with Sales and Distribution (SD) in SAP ERP
- Integration of Leasing in SAP CRM with Contract Accounts Receivable and Payable (FI-CA) in SAP ERP
- Integration of SAP CRM with SAP Utilities as part of SAP ERP

Relevant Application Objects and Available Deletion Functionality

SAP CRM uses SAP ILM to support the deletion of personal data. For more information about SAP ILM, see SAP Library for SAP ERP on SAP Help Portal at help.sap.com/erp › *<Choose relevant release>* › *Application Help* › *SAP ERP Cross-Application Functions* › *Cross-Application Components* › *SAP Information Lifecycle Management*.

For information about the relevant application objects and available deletion functionality in SAP CRM, see SAP Library for SAP CRM on SAP Help Portal at help.sap.com/crm › *<Choose relevant release>* › *Application Help* › *Basic Functions* › *Data Archiving*: *ILM Objects in SAP CRM* and *Data Destruction Objects in SAP CRM*.

Relevant Application Objects and Available EoP Functionality

For information about the EoP in SAP CRM, see SAP Library for SAP CRM on SAP Help Portal at help.sap.com/crm › *<Choose relevant release>* › *Application Help* › *Master Data* › *Business Partners* › *Functions* › *Blocking and Deletion of Personal Data in SAP CRM*.

Process Flow

1. Before archiving data, you must define residence time and retention periods in *SAP Information Lifecycle Management* (`ILM`).
2. You choose whether data deletion is required for data stored in archive files or data stored in the database, also depending on the type of deletion functionality available
3. You do the following:

- Run transaction IRMPOL and maintain the required residence and retention policies for the central business partner (ILM object: CA_BUPA).
- Run transaction IRMPOL and maintain the required residence and retention policies for the customer master and vendor master in SAP ERP (ILM objects: FI_ACCPAYB, FI_ACCRECV, FI_ACCKNVK)
- Run transaction BUPA_PRE_EOP to enable the end of purpose check function for the central business partner.
- Run transaction CVP_PRE_EOP to enable the end of purpose check function for the customer master and vendor master in SAP ERP.
- Business users can request unblocking of blocked data by using the transaction BUP_REQ_UNBLK.
- If you have the needed authorizations, you can unblock data by running the transaction BUPA_PRE_EOP and CVP_UNBLOCK_MD
- You delete data by using the transaction ILM_DESTRUCTION for the ILM objects of SAP CRM.

For information about how to configure blocking and deletion for SAP CRM, see *Configuration: Simplified Blocking and Deletion*.

Configuration: Simplified Blocking and Deletion

- You configure the settings related to the blocking and deletion of business partner master data in Customizing for *Cross-Application Components* under *Data Protection*:
  - Define the settings for authorization management under *Data Protection* › *Authorization Management*.
  - Define the settings for blocking under *Data Protection* › *Blocking and Unblocking* › *Business Partner*.
- You configure the CRM-specific settings related to the blocking and deletion of business partner master data in Customizing for *Customer Relationship Management* under *CRM Cross-Application Components* › *Data Protection*.

1.14.2 Read Access Logging

If no trace or log is stored that records which business users have accessed data, it is difficult to track the person(s) responsible for any data leaks to the outside world. The *Read Access Logging* (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data, for example, of a business partner, and in which time frame.

In RAL, you can configure which read-access information to log and under which conditions.

For more information, see *Read Access Logging* in the documentation for *SAP NetWeaver* on SAP Help Portal under help.sap.com.

1.15 Security for Third-Party or Additional Products

SAP Customer Relationship Management (SAP CRM) may be used with third-party or additional products that provide additional security features. The following products must be considered in this context:

- Hard disk encryption hardware/software is recommended for general protection of the data stored on mobile devices. The product must be distributed, installed, configured, and maintained to provide appropriate security. Therefore, appropriate security concepts, as well as technical and organizational processes must be implemented at your company.

- For providing additional communication security by using secure sockets layer (SSL) or secure network communication (SNC), appropriate cryptographic libraries or products must be installed and configured.
- Virtual private network (VPN) products may be used for protecting the communication path used by mobile or remote users (such as home office users) to connect to SAP CRM components (such as a communication station or CRM server). Appropriate security concepts as well as technical and organizational processes must be implemented at your company to operate the VPN products securely.

Depending on the usage scenario, special applications may be required.

1.16 Dispensable Functions That Impact Security

SAP Customer Relationship Management (SAP CRM) consists of several components. Some of them are necessary in specific usage scenarios only (see Technical System Landscape [page 9] and the *SAP Customer Relationship Management Master Guide* on SAP Service Marketplace at service.sap.com/crm-inst).

➡ Recommendation

Install only the required components. This reduces the risk of attacks through components that are not required, and which, therefore, may not be configured appropriately.

Depending on the usage scenario, certain functions must be deactivated or configured securely if they are not used. For more information, see the *Component-Specific Guidelines* section for the corresponding usage scenario.

1.17 Enterprise Services Security

The following sections in the *SAP NetWeaver Security Guide* and documentation are relevant for all enterprise services delivered with SAP CRM:

- *Security Guide Web Services (ABAP)* and *Security Aspects for Web Services* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for Connectivity and Interoperability Technologies*
- *Recommended WS Security Scenarios* on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security*
- *SAP NetWeaver Process Integration Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units*

1.18 Other Security-Related Information

The followin security-relevant information must be considered:

- The interaction center WebClient (IC WebClient) uses active scripting of Java applets, which requires appropriate Web browser settings. For more information, see Component-Specific Guidelines: Interaction Center [page 202].

> **Recommendation**
>
> Advise users and customers to use different trusted zones that Web browsers offer. SAP Customer Relationship Management (SAP CRM) components must be located in a trusted zone for which less restrictive security settings can be made. Users must not lower the security level of the Internet zone, because doing so makes the system more vulnerable to attacks by malicious Internet sites.

- Filtering inputs from the client. Two kinds of attacks can be attempted by hackers from this side:
    - Inclusion of malicious script code through input fields allows unauthorized users to access the Web site runtime context in the browser. Hackers can use this means, for example, to obtain a password, credit card information, and other sensitive information that is submitted to a malicious server. This vulnerability is well-known as cross-site scripting.
    - Inclusion of Structured Query Language (SQL) statements (through input fields), which could potentially be executed on the server, resulting in an unwanted or unauthorized operation.
- Session hijacking is the ability of hackers to take over the application session of another user. This can lead to serious security problems because the hacker is then in a position to act on behalf of the user, potentially accessing the user's personal information.

  The network topology between the clients and the server influences the ability of a hacker to obtain the session ID of a user, because in a noncommuted network area, all content transmitted between peer points can easily be monitored. Storing the user's IP address in the session and validating it at each user request is one way to mitigate this vulnerability. Using the Network Address Translation (NAT) protocol on the user side can, however, affect the efficiency of this solution. The secure HTTP protocol (HTTPS) also helps prevent this kind of attack.
- Hyperlinks in the *Notes* assignment block of business transactions could pose a security risk.

  In Customizing, you can specify that text patterns are interpreted as hyperlinks in the *Notes* assignment block of business transactions (for example, service requests, incidents, and problems). These hyperlinks could pose a security risk under certain circumstances, for example if hyperlinks point to a page with malicious content.

  To avoid this, you can redefine the text patterns in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* > *Text Management* > *Define Text Format* ◀. You can create a copy of the text conversion class `CL_CRM_TEXT_FORMAT_CONVERSION` and adapt the class according to your business requirements.

  In addition, you can add checking functions to the class, which are provided by SAP NetWeaver. For more information, see SAP Library on SAP Help Portal at ▶ help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Secure Programming Guide* > *Secure Programming ABAP* > *Secure User Interface* > *Canonicalization* > *Section: What Do I Get from the SAP NetWeaver Platform?* ◀.
- Smart forms in the notification framework must be used with caution.

  In the notification framework, subscriptions are connected to smart forms that are sent out to the corresponding subscribers. Note that you must not pull sensitive information using smart forms to prevent sensitive information being viewed by subscribers who are not authorized to access the information.
- Hidden inputs must be used with caution because they can be easily replaced by malicious users. If, for instance, a shopping application stores item prices in hidden inputs and if this data is used by the application on the server to calculate the transaction cost, a hacker can easily replace the prices with lower values. In

addition, the hidden inputs are not really “hidden” and can be accessed easily using the Web page source. So hidden inputs must not be used to store sensitive information.

- To guard against hackers trying to obtain users’ credentials and hijacking users’ sessions, we recommend that you use the secure HTTP protocol (HTTPS).
- Cookies must be used with caution; in particular when they are used to store sensitive information, because they can be vulnerable to different kinds of attack including cross-site scripting.
- HTTP headers (information retrieved from HTTP request headers) must be used with caution (for example, HTTP referrer header), because their content can be changed easily by using scripts or proxies.
- Since anyone can easily view the comments in the source code of the Web page, developers must be aware of comments placed in Web pages that could help potential hackers find application vulnerabilities.
- Although SAP CRM is designed to run independently of SAP NetWeaver Portal, you can integrate SAP CRM into SAP NetWeaver Portal. For information about the different integration options of SAP CRM into SAP NetWeaver Portal, see SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *WebClient UI Framework* > *Portal Integration*.

> Recommendation
>
> Although you can optionally replace the SAP NetWeaver Portal header area with the SAP CRM header area, we recommend that you use alternative configuration options, as described in *Portal Integration*.

Depending on the individual components, there may be other security-related information that should be considered or may be important. For more information, see the *Component-Specific Guidelines* section for the corresponding components.

1.19 Payment Card Security According to PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) was jointly developed by major credit card companies to create a set of common industry security requirements for the protection of cardholder data. Compliance with this standard is relevant for companies processing credit card data. For more information, see www.pcisecuritystandards.org .

This section of the security guide for SAP Customer Relationship Management (SAP CRM) supports you in implementing payment card security aspects and outlines steps that need to be considered to be compliant with the PCI-DSS. Note that the PCI-DSS covers more than the following steps and considerations. Complying with the PCI-DSS lies completely within the customer’s responsibility, and we cannot guarantee the customer’s compliance with the PCI-DSS.

Note that this guide is application-specific. For general information on ensuring payment card security, see *Payment Card Security: Security Guide* on SAP Service Marketplace at service.sap.com/securityguide > *SAP Business Suite Applications* > *Payment Card Security*.

For updated general PCI-DSS information, see SAP Note 1609917.

Payment card data in SAP CRM can be used in the following components:

- Master data
- Business transactions in the WebClient UI, for example the following business transactions:
  - Sales order
  - Sales quotation

  - Service order
  - Service order quotation
  - Service contract
  - Service contract quotation
  - Service confirmation
  - Warranty claim
  - Complaint
  - In-house repair
  - Provider order
  - Provider contract
  - Billing
  - ERP sales order
- Web Channel enablement:
  - Business-to-business (B2B)
  - Business-to-consumer (B2C)
- Partner channel management:
  - Business-on-behalf (BOB)
  - Collaborative Showroom (CSR)
  - Hosted order management (HOM)
- Enterprise services

For information about payment card processing in SAP CRM, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *Basic Functions* > *Payment Card Processing*.

1.19.1 Credit Card Usage Overview

General Information

The payment card data can be stored in an encrypted form. During data replication to SAP ERP, the system uses the decrypted payment card master data.

Payment card numbers can be displayed in masked format (`41111*********11`) or unmasked format (with a full number, such as `4111111111111111`).

The masking function depends on the activation of the payment card encryption. If the payment card encryption is active, the card number is always shown in masked format (after saving the first time) and can be displayed by authorized users only.

Standard Sales and Service Business Transactions

Payment card data can be entered in the *Payment Methods* assignment block. For specifics regarding creating and changing payment records, see the information on authorization object `CRM_ORD_PC` in the Settings for Payment Card Security [page 46] section.

The usage of payment cards in transaction types of category *Sales* can be disabled in Customizing for *Customer Relationship Management* under *Basic Functions* > *Payment Cards* > *Basic Settings* > *Assign Payment Plan Type to Transaction*.

Business Partner Master Data

Payment card data can be entered in the business partner master data, in the *Payment Cards* assignment block, and accessed during business transaction processing. If only one card is stored in the master data, this is automatically the standard card. If more than one card is stored, one card can be marked as the standard card.

Billing in SAP CRM

If payment cards are used as the payment method, the payment card data is displayed in the *Payment Cards* assignment block in the billing document, according to the system security settings. The payment card data is transmitted to accounting in SAP ERP using a Remote Function Call (RFC) connection.

ERP Sales Orders in SAP CRM

Payment card data can be entered in the *Payment Cards* assignment block in SAP CRM. Data persistence, storage, and processing logic are done in ERP Sales and Distribution. Payment cards are stored in an encrypted way and masked for display on the UI when you have made the corresponding settings in ERP Sales and Distribution. There are no settings to be made in Customizing for SAP CRM.

➡ Recommendation

- Use payment card encryption and masking. For more information, see Encryption, Decryption, and Storage of Encrypted Numbers [page 51].
- Use a separate, trusted, and SNC secured RFC connection based on the current user. For more information, see ERP Sales Document Processing [page 158].

i Note

In addition to the authorization check setup that you need in SAP ERP Sales and Distribution, the system uses the authorization object `CRM_ERP_C` in SAP ERP. When sales representatives use the input help to search for payment card numbers, the system uses this authorization object to determine if the current user is allowed to view the payment card numbers of the current sold-to party.

Web Channel Enablement

In the e-commerce scenarios, if payment card encryption is active, the masking of payment cards depends on the current user's authorizations. If a user has the authorization to decrypt payment card numbers, the payment card numbers are displayed unmasked in the Web applications (without the user having to request the unmasked display).

Service Industries Based On SAP CRM

Payment card data can be entered in the business partner master data and in the business transactions that are used in SAP for Telecommunications, SAP for Utilities, and SAP for Public Sector.

Business Agreement

You can use a business agreement to store controlling data for long-term business relationships with a business partner. The data contained in a business agreement influences processes in invoicing, contract accounts receivable and payable, taxation, and correspondence processing.

The business agreement object contains a link to the payment data (bank details and payment card data) of the business partner. The payment data of the business partner is stored in the master data, and the payment data displayed in the business agreement is retrieved from the master data.

The payment data in a business agreement is displayed according to the security settings for payment cards. If the SAP CRM system is set up to display payment card numbers in masked format, the payment card data is displayed masked in the business agreement as well.

Financial Customer Care and Dispute Management

Entering Payment Data in the Interaction Center WebClient

In the Interaction Center (IC) WebClient, you can enter payment data in a separate view (UI component `CRM_IC_PAYMENT`) and assign the payment data to business agreements of the confirmed account. You can also enter payment data in business transactions, for example sales orders.

You can use the credit card verification function to request the card verification value (CVV) for credit cards. For more information, see SAP Library on SAP Help Portal at ▶ help.sap.com/crm › *<Choose a release>* › *Application Help* › *SAP CRM for Industries* › *Utilities* › *Functions for the Utilities Industry* › *Functions for the Interaction Center (Utilities Industry)* › *Credit Card Verification* ◀.

To use the credit card verification function for business transactions, you must make settings in Customizing. For more information, see the Settings for Payment Card Security [page 46] section.

Account Balance: Entering Incoming Payment Data

The account balance for an account and the related business agreements provides the agent in the Interaction Center for Financial Customer Care with an overview of all the data on the individual business agreements, such as the open amount, due amount, and total open payments.

IC agents can receive card payments from the customer by selecting the *Credit Card* payment type and entering the selected total amount, as well as, if applicable, an amount for clarification that can be cleared, and the actual payment amount for the payment. Payment card numbers are displayed masked or unmasked, according to the corresponding system settings. IC agents can either perform online authorization or check the CVV.

IC agents can also enter new payment cards for an account and assign payment cards to business agreements. The payment card data is stored in the business partner master data unless a one-time payment card is used for the incoming payment. In the case that a one-time payment card is used, the payment card data is not stored in the business partner master data. The payment card data is sent by RFC to the connected SAP ERP back-end system and saved as a payment card supplement to the document in accounts receivable and payable.

For more information, see the following references:

- Data storage security in payment card supplement

  SAP Library for SAP ERP Central Component on SAP Help Portal at ▶ help.sap.com/ecc › *<Choose relevant release>* › *Application Help* ◀: Search for *Payment Card Security According to PCI-DSS*.

- Security regarding RFC calls between two systems

  Network and Communication Security [page 29] section

- Card verification value check

  Subsection *Creating Payment Data in the Interaction Center WebClient* above

SAP for Telecommunications: Sales and Order Management in the IC WebClient

When creating sales orders or service orders, you can assign a business agreement to the order items that contains a link to the payment data in the business partner master data. The payment data is stored in the business partner master data, not in the sales order, service order, or provider contract. For more information, see the following subsections above:

- *Business Agreement*
- *Entering Payment Data in the Interaction Center WebClient*

SAP for Utilities: IC WebClient

You can enter payment data, such as payment card information, during contract creation. The payment data is stored in the business partner master data, not in the contract.

Electronic Toll Collection: IC WebClient

You can enter payment data, such as payment card information, when creating a contract and when creating a top-up request. The payment data is stored in the business partner master data, not in the contract.

Partner channel management

Payment card data that has been entered by consumers in the Collaborative Showroom application is displayed in the hosted order management (HOM) application of partner channel management.

Loyalty Management

Note

Loyalty management does not support any security measures for credit cards. Do not use credit card numbers as loyalty membership card numbers, for example in Co-branding scenarios. If a credit card number is used as a loyalty membership card number, you must implement the required security measures for credit cards through custom-defined system enhancements, including security measures for the storage of credit card data.

1.19.2 Settings for Payment Card Security

For general information on ensuring payment card security, see *Payment Card Security: Security Guide* on SAP Service Marketplace at service.sap.com/securityguide > *SAP Business Suite Applications* > *Payment Card Security*.

The following settings are relevant for payment card security in SAP Customer Relationship Management (SAP CRM):

RFC Connections

If you want to send out decrypted payment card numbers, we recommend that you use secure network communication (SNC) encryption. For example, during data exchange of sales orders between SAP CRM and SAP ERP, the system decrypts the payment card numbers in SAP CRM and sends the payment card numbers to SAP ERP in a decrypted form. In SAP ERP, the payment card number can be encrypted again, depending on the Customizing settings.

You set up SNC in Customizing for *Customer Relationship Management* under *CRM Middleware and Related Components* > *Communication Setup* > *Define RFC Destinations*.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *Protecting Your Productive System (Change & Transport System)* > *Security for the RFC Connections* > *Secure Network Communications*.

Encryption

The SAP Cryptographic Library is the default security product delivered by SAP for performing encryption functions in SAP systems. You can use the cryptographic software provided by SAP without an additional license.

This software uses the encryption standard PKCS7. Export regulations specify that every customer needs to download the software from SAP Service Marketplace at service.sap.com. For more information about software, license determinations, and downloads, see SAP Note 597059.

To use payment card encryption, proceed as follows:

1. Install the cryptographic software provided by SAP on all application servers as described in SAP Notes 662340 and 1014619.
2. Call the *Trust Manager* (`STRUST`) transaction.
3. Create a personal security environment (PSE) for *Standard Application*. Set the algorithm to *RSA* and the recommended key length to 1024.
4. In the *Trust Manager* transaction, create a backup of the PSE by choosing *PSE* > *Export*.
5. Activate encryption in Customizing for *Customer Relationship Management* under *Basic Functions* > *Payment Cards* > *Basic Settings* > *Maintain Payment Card Type*.
6. Make the required settings in Customizing for *Customer Relationship Management* under *Basic Functions* > *Payment Cards* > *Basic Settings* > *Make Security Settings for Payment Cards*.

For more information about encryption functions in SAP systems, see SAP Note 1034482.

Encryption Checklist

Table 14

Activity	Where to Check	What to Check
Encryption is activated.	The *Trust Manager* (`STRUST`) transaction Choose *Environment* > *Display SSF Version*.	The cryptographic software provided by SAP is installed and the PSE is available on all servers. If the PSE is installed, all traffic lights under *Standard Application* are green.
Data encryption has been tested.	The *Check Encryption on Servers* (`PCA_SC`) transaction	Data encryption on all servers is functioning.
Encryption is activated for all kinds of payment cards.	In Customizing for *Customer Relationship Management* under *Basic Functions* > *Payment Cards* > *Basic Settings* > *Maintain Payment Card Type*	The *Encryption* checkbox is selected.
Masked display is functioning, and the number of visible characters for masking is set according to your requirements.	In Customizing for *Customer Relationship Management* under *Basic Functions* > *Payment Cards* > *Basic Settings* > *Make Security Settings for Payment Cards*	The payment card number is masked after saving. Check this by creating a business transaction in the WebClient UI and entering test payment card data.

Further Security Settings for Payment Cards

You can make settings for the following security-relevant aspects:

- Masked display (encryption upon saving)

> Note
>
> In an SAP CRM system, you must select the security level *Masked Display and Encrypted When Saved*.

- Additional authorization check for unmasked display (authorization object B_CCSEC)
- Visible characters for masking
- Logging of unmasked display

You do this in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *Payment Cards* › *Basic Settings* › *Make Security Settings for Payment Cards* ◀.

Standard Authorization Objects

Table 15

Authorization Object	Field	Value	Description
B_CARD_SEC	ACTVT	03_Display	Display of the decoded payment card number Searching for sales orders by payment card numbers
		06_Delete	Deletion of entries from the security area
B_CCSEC	ACTVT	03_Display	Unmasked display of payment card numbers
		06_Delete	Deletion of access logs once a certain time period has expired
		71_Analyze	Evaluation of access logs
CRM_ORD_PC (Standard sales and service business transactions only)	PR_TYPE	Business transaction type	Restriction of display and editing of payment card records to the specified business transaction types
	ACTVT	02_Change	Processing of payment card records
		03_Display	Display of payment card records

To display payment card numbers in masked format, no authorization is required. To request the display of unmasked and decrypted payment card numbers, the user must be assigned to the following authorization objects:

- B_CARD_SEC with the activity 03_Display

  This authorization enables the user to decrypt payment card numbers.
- B_CCSEC with the activity 03_Display

  You must activate the use of authorization object B_CCSEC in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *Payment Cards* › *Basic Settings* › *Make Security Settings for Payment Cards* ◀.

Recommendation

The authorization to display unmasked payment card numbers using the two authorization objects `B_CARD_SEC` and `B_CCSEC` must be granted only in the case of a compelling business need and to a limited number of key users in your company.

Specifics for Web Channel Enablement

In the e-commerce scenarios, if payment card encryption is active, the masking of payment cards depends on the current user's authorizations. If a user has the authorization to decrypt payment card numbers through authorization object `B_CARD_SEC`, payment card numbers are displayed unmasked in the Web applications, without the user having to request the unmasked display.

Authorization object `B_CCSEC` is not used in Web Channel Enablement.

Specifics for Web Services

The Web services related to sales orders are implemented in addition to the described application programming interfaces (APIs), and the same authorization objects apply.

Important SAP Notes

Table 16

SAP Note Number	Short Text
633462	Encrypt credit card data
597059	License conditions of SAP Cryptographic Library
397175	SAP Cryptographic Software - Export Control
662340	SSF Encryption Using the SAPCryptolib
1014619	Credit Card Encryption
890512	Credit card numbers are displayed in the BDOC monitor
1034482	FAQ: Credit card encryption in CRM

Specifics for Financial Customer Care and Dispute Management

You can use the credit card verification function in the Interaction Center (IC) WebClient to request the card verification value (CVV) for credit cards. To use the credit card verification function for business transactions, you must define check groups and assign the check groups to the relevant business transactions by carrying out the following steps:

- Define check groups

  You do this in Customizing for *Customer Relationship Management* under *Master Data* › *Business Partner* › *Business Agreement* › *Change Payment Data* › *Define Settings for Payment Card Check and Checking Group*.

- Assign check groups to relevant business transactions

  You do this in Customizing for *Customer Relationship Management* under *Master Data* › *Business Partner* › *Business Agreement* › *Change Payment Data* › *Define Profile for Payment Data Processing*.

In addition, you can define in the processing framework whether entering a CVV is required when creating a contract in SAP for Utilities and Electronic Toll Collection. You do this in Customizing for *Customer Relationship*

Management under ▶ *Industry-Specific Solutions* › *Utilities Industry* › *Settings for User Interfaces* › *Transaction Processing* › *Processes* › *Define Processes* ◀.

In the *Define Processes* Customizing activity, you can also define if the CVV is required only in the use of new credit cards, or also in the use of existing credit cards. Running a CVV check for existing credit cards ensures that a CVV check is carried out when existing credit card data is used for a newly created contract.

1.19.3 Rotating or Changing of Encryption Keys

You must make the following settings if you want to use rotating or changing of encryption keys:

- To use key versions and key replacement, you must activate business function *Periodic Key Replacement for Payment Card Encryption* (`PCA_KEYV`).
- Activate the key replacement function in Customizing for *Customer Relationship Management* under ▶ *Cross-Application Components* › *Payment Cards* › *Basic Settings* › *Make Security Settings for Payment Cards* ◀.
- Create key versions in the `SSFVA` transaction.

1.19.4 Masked or Unmasked Display

General Information

The masking function depends on the activation of payment card encryption. If payment card encryption is active, the card number is always shown in masked format (after saving the first time). The first four and the last two digits of the payment card number are masked. You can define the visible characters for masking in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *Payment Cards* › *Basic Settings* › *Make Security Settings for Payment Cards* ◀.

If a card number is masked, the user can request an unmasked display. For more information, see the authorization object details in the Settings for Payment Card Security [page 46] section.

The unmasked display of payment card numbers can be logged. For more information, see the Logging of Payment Card Number Access [page 51] section.

Specifics for Sales and Service Business Transactions

If payment card encryption is inactive, the appearance of card numbers depends on the user's authorizations for object `CRM_ORD_PC`. This behavior only applies to sales and service business transactions. The billing and master data components do not use authorization object `CRM_ORD_PC`.

The following table shows the authorizations that are controlled with authorization object `CRM_ORD_PC`:

Table 17

Field `ACTVT`: Value `02_Change`	Field `ACTVT`: Value `03_Display`	Use in Online Transactions
+	+	The user can change the payment card data and the card number is displayed completely (unmasked).

Field ACTVT: Value 02_Change	Field ACTVT: Value 03_Display	Use in Online Transactions
+	-	The user can change the payment card data. After saving, the payment card number is displayed in masked format.
-	+	The user cannot change the payment card data, but can see the payment card number in unmasked format.
-	-	The user cannot change the payment card data, and the payment card number is shown in masked format.

Specifics for Web Channel Enablement

In the e-commerce scenarios, if payment card encryption is active, the masking of payment card numbers depends on the current user's authorizations. If a user has the authorization to decrypt payment card numbers (authorization object B_CARD_SEC), all card numbers are displayed unmasked in the Web applications, without the user having to request the unmasked display. Authorization object B_CCSEC is not used.

1.19.5 Logging of Payment Card Number Access

If the card number is masked, the user can request an unmasked display. You can log user access to unmasked payment card data to track which user displayed which card number at which time. You activate the log in Customizing for *Customer Relationship Management* under ▸ *Basic Functions* › *Payment Cards* › *Make Security Settings for Payment Cards* ◂.

You can use report RCCSEC_LOG_SHOW or transaction CCSEC_LOG_SHOW to display the access log. To display the access log, you require authorization for the activity 71 of authorization object B_CCSEC.

You can delete log records if they are at least one year old. You do this using report RCCSEC_LOG_DEL or transaction CCSEC_LOG_DEL. To use the deletion report, you require authorization for the activity 06 of authorization object B_CCSEC .

1.19.6 Encryption, Decryption, and Storage of Encrypted Numbers

Setting Up Encryption

For information about setting up encryption, see the Settings for Payment Card Security [page 46] section.

Data Storage Security

If you use payment card encryption, it is encrypted with the cryptographic software provided by SAP and forwarded to the database.

Encryption is also supported if business transaction data is exchanged with the ERP back-end system. Payment cards can be encrypted in both systems, only in one system (SAP Customer Relationship Management (SAP CRM) or SAP ERP), or in neither system. If the masking function is active in SAP CRM, the card number is stored internally and in masked form in a business document (BDoc) that is required for data exchange with SAP ERP.

For more information about payment card encryption in SAP ERP, see SAP Notes 766703 and 633462.

Specifics for Sales Applications, Service Applications, and Billing

If encryption is active, the payment card numbers are stored in masked form in the `COMD_PAYPLAN*` database tables.

Data Protection

For privacy protection, we recommend that you store payment card numbers in the database in encrypted format. Furthermore, any card number must be masked if it is displayed on the user interface (UI) or printed out in documents.

1.19.7 Migration

If you want to encrypt existing payment information for a migration, refer to SAP Note 896819. To encrypt existing data, you can use report `CRM_ORDER_PC_RETROGR_ENCRYPT` or report `PCA_MASS_CRYPTING`.

> **Note**
>
> Card numbers encrypted retroactively are not masked.

1.19.8 Archiving

Generally, only masked credit card information can be archived. Clear text credit card information must not be archived. Archiving encrypted credit card information must not be done because archived data must not be changed. Encrypted credit card information has to be re-encrypted with a different key, for example, with key rotation, as required by PCI-DSS. This change of data is not possible in an archive. In technologies that are agnostic to the semantics of the data, such as Process Integration (PI), ABAP Web Services, or Forward Error Handling (FEH), archiving has to be disabled. IDocs that contain credit card information must not be archived.

For information about archiving, see SAP Library for SAP ERP Central Component on SAP Help Portal at help.sap.com/ecc › *<Choose relevant release>* › *Application Help*: Search for *Archiving of Encrypted Payment Card Data*.

Specifics for Sales Applications, Service Applications, and Billing

The archiving of data related to payments (tables `COMD_PAYPLAN*`) does not involve additional encryption or decryption. If encryption is active, the payment card numbers are stored in masked form in the `COMD_PAYPLAN*` database tables, and the payment data is archived in the form in which it has been stored in the database tables.

1.19.9 Interfaces (IDoc/Services)

Network and Communication Security

On the WebClient UI, we recommend that you use HTTPS encryption to protect the data.

If you want to send out decrypted payment card numbers, we recommend that you use secure network communication (SNC) encryption. For example, during the data exchange of sales orders between SAP CRM and SAP ERP, the system decrypts the payment card numbers in SAP CRM and sends the payment card numbers to SAP ERP in a decrypted form. In SAP ERP, the payment card number can be encrypted again, depending on the Customizing settings.

For information about setting SNC, see the Settings for Payment Card Security [page 46] section.

Card Verification Values

⚠ Caution

Do not process asynchronous services that contain a card verification code or value data (`CAV2`, `CID`, `CVC2`, `CVV2`). Note that in SAP's approach to service-oriented architecture (SOA), these values correspond to global data type (GDT) `PaymentCardVerificationValueText`. The payload of asynchronous services is persisted in the database until the service is processed, and it is not allowed to persist card verification values (CVV) according to PCI-DSS. Synchronous services can be processed because their payload is not persisted.

The following asynchronous services must not be used:

- `SalesOrderCRMChangeRequest_In`
- `SalesOrderCRMConfirmation_Out`
- `SalesOrderCRMCreateRequest_In`
- `SalesOrderCRMNotification_Out`
- `CustomerCRMCreateRequest_In`
- `CustomerCRMChangeRequest_In`
- `CustomerCRMConfirmation_Out`

Forward Error Handling

⚠ Caution

In SAP Customizing, disable Forward Error Handling (FEH) for all services that contain credit card numbers.

IDoc Processing

IDoc segments cannot store credit card numbers in clear text due to the PCI security standard compliance. Once an IDoc is being processed within the IDoc Framework, all values are temporarily stored, including the clear text credit card number. For more information about how to process IDocs containing credit card information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for Connectivity and Interoperability Technologies* > *Security Guide ALE (ALE Applications)*.

1.19.10 RFC Debugging

⚠ Caution

Disable RFC debugging when you process credit card information in a productive system. Do not activate the *Set RFC Trace* option in your productive system. If this option is active, the system saves all input data of an RFC call in clear text to a file. If credit card numbers (PAN) are included in calls to function modules, the data is also stored in the file. Since these numbers have to be stored encrypted according to the PCI-DSS standard, activating this option results in no longer being PCI-DSS compliant.

1.20 Trace and Log Files

Trace files and log files can become significant security weaknesses of applications if some basic precautions, such as the following, are neglected:

- Applications must use the SAP standard logging and tracing application programming interface (API) and the application server (AS) Java mechanism. Besides the fact that the AS Java manages the access and protection of log files and trace files, there are other advantages that justify its use:
    - It avoids the need for coding the same function twice.
    - It avoids potential performance problems arising from customer implementation.

  For more information, see SAP Solution Manager.
- Applications must make sure that the log file does not contain any sensitive information including, but not limited to:
    - User logon information, such as a password
    - Credit card information
    - Remote function call (RFC) traces of sensitive import/export parameters
- Applications must set the trace level to the minimum value so that minimal information is included in the log file.
- Tracing must be switched off in a production environment, because tracing content is intended, primarily, to help developers and the support team.

While trace and log files can reveal important information to potential intruders, they can also be used by the system administrator to log important user activities. We recommend that you start creating activity logs and monitor them proactively to detect potential attacks. Once an attack occurs, it is too late to generate logs.

To ensure that log files are available when required, they must be backed up.

SAP CRM supports the logging and tracing mechanisms provided by SAP NetWeaver. For more information, see the following sections in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* :

- *Security Aspects for Lifecycle Management* › *Auditing and Logging*
- *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for the Application Server* › *Security Guides for the AS Java* › *SAP NetWeaver Application Server Java Security Guide* › *Tracing and Logging*

1.21 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 EarlyWatch 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 SAP Notes if possible. If you cannot implement the SAP 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 SAP Solution Manager, as a remote service, or as an on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation for a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance with 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 existence 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 a 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 information about these services, see:

- EarlyWatch Alert: service.sap.com/ewa
- Security Optimization Service / Security Notes Report: service.sap.com/sos

- Comprehensive list of Security Notes: service.sap.com/securitynotes
- Configuration Validation: service.sap.com/changecontrol
- RunSAP Roadmap, including the Security and the Secure Operations Standard: service.sap.com/runsap (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)

2 Component-Specific Guidelines: Master Data

2.1 Accounts and Contacts

Why Is Security Necessary?

Security within account, contact, and employee processing in the master data area is necessary because these areas access sensitive customer and personal data, such as private address data, payment cards and bank details, and so on. These data accesses are made from one central point that is integrated automatically into the different systems (such as SAP ERP back end or mobile clients). Therefore, you should restrict access to this data.

User Administration and Authentication

User Management

Table 18

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialog user	No	Obligatory user who can access service transactions. To be maintained by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Obligatory user who can process background tasks. To be maintained by an SAP CRM system administrator.
SAP NetWeaver Business Warehouse (SAP NetWeaver BW)	Personal user	No	Dialog user	No	Obligatory user who can access SAP NetWeaver BW applications. To be maintained by an SAP CRM system administrator.
SAP ERP	Personal or technical user	No	Dialog or system user	No	Obligatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, user can be a personal user or a system RFC user. To be maintained by an SAP ERP system administrator.

User Management Tools

Table 19

Tool	Description
User Maintenance (transaction SU01)	For more information, see User Administration and Authentication [page 18].

User Types

The personal user type is used to create users such as the following:

- Dialog users
- Background users

Customers must create the following users:

- Individual users so that they can use the standard processes that are delivered
- Initial identification parameters, such as the password and certificate for the users

Authorizations

Account, contact, and employee processing uses the authorization technique provided by SAP NetWeaver Application Server (SAP NetWeaver AS). Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the application.

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

For the description of the authorization procedure used in SAP CRM master data processing, see Component-Specific Guidelines: SAP CRM [page 68].

The following authorization objects and authorization fields are used for account, contact, and employee processing:

Standard Authorization Objects

Table 20

Authorization Object	Authorization Fields
B_BUPA_FDG (Business Partner: Field Groups)	ACTVT FLDGR (Field group for authorization)
B_BUPA_GRP (Business Partner: Authorization Groups)	ACTVT BEGRU (Authorization group)
B_BUPA_RLT (Business Partner: BP Roles)	ACTVT RLTYP (BP role)
B_BUPR_BZT (Business Partner Relationships: Relationship Categories)	ACTVT RELTYP (Business partner relationship category)
B_CARD_SEC (Authorization Encryption Card Master)	ACTVT
B_CCARD (Payment Cards)	ACTVT
UIU_COMP (UIU: Component Access Authorization Check)	COMP_NAME (Component Name) COMP_WIN (Component Window Name)

Authorization Object	Authorization Fields
	COMP_PLUG (Inbound Plug)
CRM_BPROLE (CRM Business Partner: BP Roles)	ACTVT BPROLE (BP Role)
S_USER_GRP (User Master Maintenance: User Groups)	CLASS (User group in user master maintenance) ACTVT
SMI_AUTH (Social Media Intelligence Authorization)	SMI_ACTVT (Processing Type)

Additional Authorization Checks

Enhanced authorization check capabilities related to the secured processing of sensitive data of accounts, contacts, and employees in SAP CRM are provided by the *Authorization Checks* (BADI_CRM_BP_UIU_AUTHORITY) Business Add-In (BAdI). For more information, see the BAdI documentation.

Network and Communication Security

The network topology for master data is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and the corresponding section of Component-Specific Guidelines: SAP CRM [page 68] also apply to CRM master data.

For more information, see Network and Communication Security [page 29].

Communication Channel Security

The following communication channels are used:

- Remote function call (RFC)
- Business document (BDoc) types: BUPA_MAIN, BUPA_REL, BUHI_MAIN, BUPA_KNVH, VEND_MAIN
- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Table 21

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive CRM data such as payment card information, customer data, and employee data
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as payment card information, customer data, and employee data
CRM server to ERP server	RFC	System ID, client, and host name, all application data	System information and CRM data

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
ERP server to CRM server	RFC	System ID, client, and host name, all application data	System information and ERP data
CRM server to SAP NetWeaver BW server	RFC	System ID, client, and host name, all application data	System information and CRM data
CRM server to third-party supplier (Transaction Tax Engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data

Data Storage Security

The data is stored in database tables owned by the CRM application and SAP NetWeaver AS. Depending on the user, rights such as read, write, change, and delete are required. There is no need for a special data storage security handling. The security of sensitive data such as payment card numbers can additionally be protected by using encryption. For more information about payment card number encryption, see section Payment Card Security According to PCI-DSS [page 42].

2.2 Assortments

Security within assortment maintenance in the master data area is necessary because assortments are used to maintain sensitive data such as customer-specific listings. In addition, creating or editing erroneous assortments has an impact on business execution. From one central point, changes can be distributed automatically to different systems. This is why you should restrict access to this data.

User Administration and Authentication

User Management

Table 22

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialog user	No	To be maintained by an SAP CRM system administrator

User Management Tools

Table 23

Tool	Description	Prerequisites
User and role maintenance with SAP NetWeaver AS ABAP (transactions `SU01` and `PFCG`)	For more information, see User Administration and Authentication [page 18].	None

User Types

The personal user type is used, such as:

- Dialog users
- Background users

To use the standard processes that are delivered, customers must create individual users.

Authorizations

Assortment maintenance uses the authorization technique provided by SAP NetWeaver Application Server (SAP NetWeaver AS). Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the application.

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

For the description of the authorization procedure used in CRM master data processing, see Component-Specific Guidelines: SAP CRM [page 68].

The following authorization objects and authorization fields are used for assortment maintenance:

Standard Authorization Objects

Table 24

Authorization Object	Authorization Fields	Values	Description
`CRM_PRP_MT`	`ACTVT`	01 Create (including change) 02 Change (including display) 03 Display	Type of change

	`PPR_TYPE`	`0001 Purchase Contracts`
		`0002 Product Catalog View`
		`0003 Sales Contracts (internal)`
		`0004 Service Contracts`
		`0008 Top n Product List`
		`0009 Channel Commerce`
		`0010 Sales Contracts`
			Type of Partner/Product Range (PPR)
			The PPR controls the properties of the partner/product range, for example:
			• The scenario, such as Internet or Sales, to which they apply
			Or
			• The objects, such as partner, function, sales,

Authorization Object	Authorization Fields	Values	Description
		0011 Service Recall 0012 Marketing Project 0020 Proposal for Activity Template 0030 Service Product List 0ACP Account Planning Responsibility 0DRG CMS Design Registration: PPR Type 0ML Mandatory Listing 0OL Optionals Listing 0PL Promotional Listing 0PLN PPRfor Planogram	and so on, to which they apply. **Dependencies** You specify the PPR type in Customizing. Note Top n list is automatically set as a PPR for this type of list.
	PPR_APPLIC	ASMT	N/A

Network and Communication Security

The network topology for master data is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and the corresponding section of Component-Specific Guidelines: SAP CRM [page 68] also apply to CRM master data.

For more information, see Network and Communication Security [page 29].

Communication Channel Security

The following communication channels are used:

- Business document (BDoc) type (for data exchange with mobile client): partner/product range (PPR)
- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Table 25

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords and all sensitive CRM data

2.3 Listings

Why Is Security Necessary?

The system accesses sensitive data such as customer-specific listings or exclusion data. In addition, creating or editing erroneous listings or exclusions has an impact on the business execution. From one central point, changes can be distributed automatically to different systems (such as SAP ERP or mobile clients). This is why access to this data should be restricted.

The listing object comprises two objects: the condition record for the listing header and the product/partner ranges (PPR) record for the listing items.

The authorization check for a listing object is performed on listing header level only; there is no additional authorization check on item level. The authorization check for the listing header is also used for the following listing reports:

- *Listed Products by Account*
- *Listings by Account Hierarchy*
- *Listings by Product Hierarchy,*
- *Non-listed Products by Account.*

For listing header records, condition technique usage LI (*Listing & Exclusion*) is used. This is the only difference compared to condition records that are used for price maintenance (usage PR). For more information about the authentication concept and related objects, see Conditions (Prices) [page 64].

Products are grouped based on the category they belong to and are displayed in the form of a hierarchy in the selection user interface. A user can list the items in this user interface. In the maintenance user interface and with the required authorizations, the user can add products that are not yet available in the selection interface.

Standard Authorization Objects

Table 26

Authorization Object	Authorization Fields	Value	Usage
`COM_PRD`	`ACTVT`	`03`	Displaying products in the selection user interface
`COM_CAT`	`ACTVT`	`03`	Displaying categories in the selection user interface
`CRM_LSTPRS`	`ACTVT`	`01`	• Displaying products, for which the user is the employee responsible, in the maintenance user interface If this authorization is not assigned, the user can only list products in the selection user interface. • Adding products in the maintenance user interface

Authorization Object	Authorization Fields	Value	Usage
CRM_LSTPRS	ACTVT	02	• Displaying all listed products in the maintenance user interface, including the products, for which the user is the employee responsible • Editing the product data

2.4 Conditions (Prices)

Why Is Security Necessary?

Security within price processing in the master data area is necessary because the system accesses sensitive data such as customer-specific discounts and conditions. In addition, creating or editing erroneous prices or discounts has an impact on the business execution. From one central point, changes can be distributed automatically to different systems (such as SAP ERP back end for trade promotion management or mobile clients). Therefore, you should restrict access to this data.

Important SAP Notes

Table 27

SAP Note Number	Short Text	Comment
986344	Release by authorization in condition records	Introduction of the authorization workflow concept for the release of condition records.
1010475	Release by authorization in condition records II	An addition to SAP Note 986344
634747	Authorization check for condition maintenance	Introduction and brief description of the role and authorization object for condition maintenance

User Administration and Authentication

User Management

Table 28

System	User	Delivered ?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialogue user	No	To be maintained by an SAP CRM system administrator
SAP ERP	Personal or technical user	No	Dialogue or system user	No	Obligatory user used for data exchange between SAP CRM and SAP ERP. Dependent upon

System	User	Delivered ?	Type	Default Password	Description
					remote function call (RFC) destination.

User Management Tools

Table 29

Tool	Description
User Maintenance (transaction SU01)	For more information, see User Administration and Authentication [page 18].

User Types

The personal user type is used to create users such as the following:

- Dialog users
- Background users

Customers must create individual users to use the standard processes that are delivered.

Authorizations

Condition maintenance (price maintenance) processing uses the authorization technique provided by SAP NetWeaver Application Server (SAP NetWeaver AS). Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the application.

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

For the description of the authorization procedure used in CRM master data processing, see Component-Specific Guidelines: SAP CRM [page 68].

The following roles, authorization objects, and authorization fields are used for condition maintenance (price maintenance):

Standard Roles

The standalone condition maintenance is included in several WebClient UI roles (for example SALESPRO, SERVICEPRO, TPM_PRO) and condition maintenance is embedded in objects such as products, business partners, contracts, trade promotions, and so on. Consequently condition master data is visible in different UI roles and objects either as a standalone application, or as an assignment block, or as a query result list. The UI role configuration and authorization assignment controls access to condition master data. The table below shows the standard PFCG role that is used by the condition maintenance.

Table 30

Role	Role Description
SAP_CRM_CONDITION_MAINTENANCE	Based on authorization object /SAPCND/CM for all activities of condition maintenance

Note

The visibility and extent to which you can edit conditions is also dependent on the setup and assignment of condition maintenance groups in Customizing.

Only those condition types and tables assigned to a condition maintenance group are visible in the WebClient UI applications. You can restrict access to condition master data in the business object specific assignments of condition maintenance groups and in Customizing for:

- *Customer Relationship Management* › *Master Data* › *Conditions and Condition Technique* › *Condition Technique: Basics* › *Create Maintenance Group*

and

- *Customer Relationship Management* › *Master Data* › *Conditions and Condition Technique* › *Condition Technique: Basics* › *Define Maintenance Group for Context*

⚠ Caution

In an integrated scenario with an SAP ERP back end system you can download conditions from SAP ERP to SAP CRM but condition types defined in SAP ERP are not assigned to any condition maintenance group delivered by SAP CRM. SAP ERP condition master data is only visible in SAP CRM when you assign the SAP ERP condition types and tables to the condition maintenance groups in SAP CRM. Therefore, you can use the assignments to restrict visibility of condition master data. The extent to which you can edit condition master data originating from SAP ERP is controlled by the Customizing in SAP ERP in the activity *Integration with Other mySAP.com Components* › *Customer Relationship Management* › *Basic Functions* › *Data Exchange Conditions*. These settings are synchronized with SAP CRM via the condition Customizing download.

Standard Authorization Objects

Table 31

Authorization Object	Authorization Fields
`/SAPCND/CM` (for condition maintenance main activities)	`ACTVT` `/SAPCND/AP` (Application as Condition Technique) `/SAPCND/US` (Usage for Condition Technique) `/SAPCND/CT` (Condition Table) `/SAPCND/TY` (Condition Type)
`/SAPCND/RC` (for condition maintenance approval workflow – see SAP Note 986344)	`ACTVT` `/SAPCND/AP` (Application as Condition Technique) `/SAPCND/US` (Usage for Condition Technique) `/SAPCND/CT` (Condition Table) `/SAPCND/TY` (Condition Type)

i Note

Condition maintenance is also enabled for the Access Control Engine (ACE). For more information, see Access Control Engine [page 324] and the Customizing activity *Customer Relationship Management* › *Basic Functions* › *Access Control Engine*. The relevant ACE object type and superobject is `CONDITIONCRM`Use the ACE to define rules to match your internal organizational structures and restrict the visibility and editing of condition records.

Additional Authorization Objects for Administrative Tasks for Condition Technique

Table 32

Authorization Object	Authorization Fields
`/SAPCND/CC` (for condition technique cross-client configuration)	`ACTVT` `/SAPCND/AP` (Application as Condition Technique) `/SAPCND/US` (Usage for Condition Technique) `/SAPCND/CT` (Condition Table)
`/SAPCND/SS` (for condition technique system settings)	`ACTVT`
`/SAPCND/CO` (for condition technique field catalog and condition table definition)	`ACTVT`

Network and Communication Security

The network topology for master data is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and the corresponding section of Component-Specific Guidelines: SAP CRM [page 68] also apply to CRM master data.

For more information, see Network and Communication Security [page 29].

Communication Channel Security

The following communication channels are used:

- Remote function call (RFC)
- Business document (BDoc) types: `CND_M_SUP`, `CMBCRMPR*` (* = name of the SAP or customer-specific condition table)
- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Table 33

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive CRM data such as prices and discounts
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as prices and discounts
CRM server to ERP server	RFC	System ID, client, and host name; all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client, and host name; all application data	System information and ERP data

3 Component-Specific Guidelines: SAP CRM

Standard SAP Customer Relationship Management (SAP CRM) focuses on the requirements of corporate in-house employees. It supports the entire customer interaction cycle starting with the first customer contact, through to business transactions, order fulfillment, customer service, and finally to analysis and reporting.

This section provides specific security information for the following key capabilities:

- Marketing
- Sales
- Service

Why Is Security Necessary?

SAP CRM consists of various applications based on SAP NetWeaver. Most of the scenarios are implemented with SAP CRM and contain all the information used in customer interactions (that is, business partners, orders, marketing projects, service contracts, and so on).

Security of SAP CRM is important because any business-related information can be accessed from this part of the implemented scenario.

Authorizations

The authorization check in SAP CRM sales and SAP CRM service and analytics occurs in the following sequence:

- Customer documents (authorization object: `CRM_ORD_OP`)
- Visibility in the organization model (authorization object: `CRM_ORD_LP`)
- Visibility in territory (authorization object `CRM_ORD_TE)`
- Combination of several authorization objects

  If the first two checks are not successful, combinations of different authorization objects are checked. All the checks must be successful before a user can process the required transaction. This means that the user must be authorized to:

  - Process the leading business transaction category in the corresponding transaction type
  - Process the corresponding transaction type
  - Process in the corresponding sales area:
    - Authorization objects per area
    - Authorization object of the transaction type (`CRM_ORD_PR`)
    - Authorization object of allowed organizational units (`CRM_ORD_OE`)

For more information about the authorization objects that are used and authorization fields, see the specific sections of this guide that deal with individual key capabilities.

For more information, see SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Basic Functions* › *Business Transaction* › *Authorization Check in Business Transactions*.

Conditions in Business Transactions

Display of individual conditions, for example, specific discounts in business transactions when using the WebClient UI can be restricted using the enhancement spot `CRM_PRCIL_ENHANCEMENT`.

Data Storage Security

Data is stored in the CRM database. The data access types include:

- Read
- Write
- Delete
- Change
- Query

Credit card information can be stored in encrypted format if cryptographic software provided by SAP is installed. For more information about credit card encryption, see section Payment Card Security According to PCI-DSS [page 42].

Security for Additional Applications

The ActiveX control is packaged in a CAB file and uploaded to the Multipurpose Internet Mail Extensions (MIME) repository of the server. The first time the calendar application runs, the ActiveX control is downloaded and installed automatically.

Prerequisites

- The user's Web browser settings allow automatic download of the ActiveX control.
- The Web browser security level is set to medium.
- The user has rights to make registry entries.

For more information, see Calendar (ActiveX) Control [page 322].

Checklist

Table 34

Feature	Check	How to Check
Credit card encryption	See the checklist in the Settings for Payment Card Security [page 46] section.	See the checklist in the Settings for Payment Card Security [page 46] section.
Calendar ActiveX control requirements	Do the user's Internet Explorer (IE) settings allow automatic download and run of signed ActiveX control?	In your Web browser, choose *Tools* > *Internet Options* > *Custom Level*. Select the *Download signed ActiveX controls* and the *Run ActiveX controls and plug-ins* radio buttons.
	Does the user have rights for making registry entries?	Microsoft Windows Authorization Tool
Credit check	What destination is used for a credit check?	See Customizing for *Customer Relationship Management* under *CRM Middleware and Related Components* > *Communication Setup* > *Middleware Parameters* > *Define Middleware Parameters*.
	What logon procedure is used for this destination?	Transaction *Configuration of RFC Connections* (`SM59`)

3.1 Marketing

3.1.1 Product Proposals

Product proposals consist of cross-selling, up-selling, down-selling, accessories, and top n lists. They use SAP NetWeaver Application Server (SAP NetWeaver AS) and SAP NetWeaver Business Warehouse (SAP NetWeaver BW).

The functionality comprises object maintenance, for example, creation of cross-selling rules and of the usage of the generated product proposal, for example, in an Internet Shop. Object maintenance functionalities are available for:

- Cross-/Up-/Down-Selling Rules (Association Rules)
- Accessories (part of product maintenance)
- Top N Lists

The generated product proposals are used in:

- Internet Sales
- Interaction Center
- Sales

User Administration and Authentication

Product proposals use the normal user management of SAP NetWeaver AS and require dialog users. If product proposals are used in Internet sales, Internet users are also required.

Product association rules for cross-selling, up-selling and down-selling, and products for top n lists can be determined in SAP NetWeaver BW and uploaded to SAP Customer Relationship Management (SAP CRM). This action requires a remote function call (RFC) connection with a user and password.

Standard Users

Table 35

System	User	Delivered?	Type	Default Password
SAP CRM	Normal user	No	Dialog user	Arbitrary
SAP NetWeaver BW	Normal user	No	Dialog user	Arbitrary

Standard Roles

Table 36

Business Role	PFCG Role	Description
MARKETINGPRO	SAP_CRM_UIU_MKT_PROFESSIONAL	Marketing Professional
ECO-MANAGER	SAP_CRM_UIU_ECO_MANAGER	E-Commerce Manager

Standard Authorization Objects

Table 37

Authorization Object	Description
CRM_PAR	Authorization Object: Product Association Rules This authorization object manages the authorization requirements for maintenance of product association rules (cross-selling, up-selling, and down-selling). It manages authorization for the following activities: • Creating new rules • Changing existing rules • Deleting existing rules • Activating existing rules If the authorizations are not maintained for a user, the user can search, and view product association rules but cannot create, change, delete, or activate rules.
CRM_PRP_MT	Authorization Object for PPR Maintenance via PRP API. This authorization object manages the authorization requirements for maintenance of top n lists. Field PPR_APPLIC = TOPN parameters manages the authorization requirements for maintenance of top n lists. Field PPR_TYPE = 0008 manages the authorization for the following activities: • Creating new top n lists • Changing top n lists • Displaying top n lists

Communication Channel Security

Table 38

Communication Path	Protocol Used	Type of Data Transferred
Frontend client using SAP GUI for Windows to application server	DIAG	Application data, for example cross-selling rules or Customizing
Frontend client using a Web browser to application server	HTTP / HTTPS	Application data, for example, cross-selling rules
Application server to application server	RFC	Cross-selling rules or Top N lists

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the Communication Channel Security section above:

Table 39

Destination	Delivered	Type	User Authorizations	Descriptions
SAP Netweaver AS	NO	DIAG	User, password	Object maintenance and product proposal usage
SAP Netweaver BW	NO	RFC	User, password	Retrieval of cross-selling rules and Top N lists

Checklist

Table 40

Feature	Check	How to Check
Creation or changing of product association rules	User settings for the `CRM_PAR` authorization object	Check user settings
Creation or changing of top n lists	User settings for the `CRM_PRP_MT` authorization object	Check user settings

3.1.2 External List Management

External list management (ELM) is built on the following components:

- SAP NetWeaver Application Server (SAP NetWeaver AS)
- SAP NetWeaver Business Warehouse (SAP NetWeaver BW)

For more information about the security aspects of the individual components, see the *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* .

User Administration and Authentication

User Management

The application uses two types of users: dialog users and workflow users.

Dialog users can create and maintain external lists (create external lists, mark the process steps that must be executed in the workflow, delete external lists, and so on).

Workflow users execute the marked process steps in ELM in the background using a workflow.

Standard Users

Workflow user `WF-BATCH` is delivered as part of the standard system (not by the application directly, but by SAP Business Workflow); if it is missing, the workflow user can be created when making Customizing settings for SAP Business Workflow.

Integration with Single Sign-On Environments

Integration with Single Sign-On (SSO) is managed by the framework and not by the application. For more information, see the *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide*.

Authorization Objects

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

The SAP NetWeaver AS authorization concept is based on assigning authorizations to users depending on roles. For role administration, use the profile generator (transaction PFCG) in SAP NetWeaver AS ABAP and the user management engine's user administration console for SAP NetWeaver AS Java. The following table lists the authorization objects:

Table 41

Authorization Object	Field	Description
CRM_LIST_H	ACTVT	CRM Marketing: External List Management
CRM_MAP_FM	ACTVT	Authorization object for CRM MKT mapping tool
SAP NetWeaver BW: S_TCODE for ELM transaction	N/A	N/A

Network and Communication Security

Communication Channel Security

The following communication channels are used by ELM:

Table 42

Communication Path	Protocol Used	Type of Data Transferred
SAP NetWeaver BW to SAP Customer Relationship Management (SAP CRM	Remote function call (RFC)	General data
Front end to application server	HTTP HTTPS RFC DIAG File system	External list file

Communication Destinations

The application does not deliver any RFC destinations or server groups. Customers must create the RFC destinations and server groups (used in parallel processing while executing process steps).

Data Storage Security

The application uploads the external list file from the front end to the application server or uses the files already stored on the application server. These files contain business partner master data. The files are stored in the MARKETING_FILES logical path in the application server.

➡ Recommendation

The physical path assigned to this logical path must have a sufficient access control mechanism.

3.1.3 Marketing Prospects

Marketing prospects consist of the address data of an individual: name, address, and e-mail address. This data is created using the external list management (ELM) component and can be used in campaign execution. The marketing prospects application is built on the SAP NetWeaver Application Server (SAP NetWeaver AS).

User Administration and Authentication

User Management

The application uses two types of users: dialog users and workflow users.

Workflow users create and delete marketing prospects using the ELM application. Dialog users can search, view, and delete the marketing prospect data using the marketing prospects application.

User

Table 43

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	No	To be maintained by an SAP CRM system administrator

Authorization Objects

The authorization object `CRM_HV_MC` controls the create, display, and delete authority for a user.

3.1.4 Segmentation

Business partner segmentation provides a range of functions that help you divide your customer base according to the marketing activity at hand.

Segmentation users need extensive authorizations. Assign only the minimum required authorization.

Important SAP Notes

Table 44

SAP Note Number	Short Text
742126	RSCRM - Necessary Authorizations
315094	Recommendations for Authoriz. in BW Reporting
697572	Additional Information on the Segment Builder Applet

SAP Note Number	Short Text
1334838	Additional information on the Flash-based Graphical Modeler

Security Aspects of Data, Data Flow and Processes

This application uses various types of personal data to compile lists of Business Partners, that is Target Groups. When Target Groups are displayed, the user sees confidential data relating to these Target Group members. Consequently, appropriate user authorizations must be maintained. With regard to the display of Target Group Items, appropriate Access Control Engine (ACE) rules must also be maintained for the corresponding Business Partners.

Target Groups can be exported to a file on the application server, and it must be ensured that only users with the appropriate authorizations can access these files that contain confidential data. Tools used to process this information must also meet security requirements.

Data must be deleted after use; deletion is not carried out in the SAP CRM system, since this is not involved in the follow-up process but must be handled by those processes.

User Management

Segmentation uses the SAP NetWeaver AS normal user management and requires dialog users. For segmentation of data stored in different systems, RFCs are used. RFC connections require both a user and a password. In Customizing for *Customer Relationship Management*, the user and password combination can be defined as the current dialog user, so that individual authorizations can be defined. If you are working with an RFC default user, you cannot define individual authorizations.

If you are carrying out segmentation with a high data volume based on data from SAP NetWeaver Business Warehouse (SAP NetWeaver BW), the user in the SAP NetWeaver BW system must have the same user name as the corresponding user in the SAP CRM system. The RFC connection that is used to connect the SAP CRM system with the SAP NetWeaver BW system has to be a trusted one.

Standard Users

Table 45

System	User	Delivered	Type	Default Password
SAP CRM	Normal User	No	Dialog User	Arbitary
SAP NetWeaver BW	Normal User	No	Dialog User	Arbitrary

Standard Roles

Table 46

Business Role	PFCG Role	Description
MARKETINGPRO	SAP_ CRM_UIU_MKT PROFESSIONAL	Marketing Professional

Other Related Roles

For the Collaborative Campaign Management Scenario

Table 47

Business Role	PFCG Role	Description
CHM-CM	SAP CRM_UIU_CHM_CHANNELMANAGER	Channel Manager
CHM-PM	SAP CRM_UIU_CHM_PARTNERMANAGER	Partner Manager

Role and Authorization Concept of Segmentation

The standard role for segmentation is the Marketing Professional, comprising all the required authorizations for the required functions.

> **Note**
>
> Segmentation is also used in the channel scenario for Collaborative Campaign Management; the roles Channel Manager and Partner Manager contain the authorizations for the use of segmentation but the Partner Manager role only comprises restricted access to Target Groups. To give the Partner Manager role full access, you must maintain the ACE Authorization as required.

Standard Authorization Objects

Table 48

Authorization Object	Field	Description	Usage
CRM_SEGTYP	ACTVT TYPE_ID	Usage	All segments can be protected with a standard SAP authorization object CRM_SEGTYP. According to the selected usage of the profile set, all subobjects (profiles, target groups, and subprofile sets) inherit this setting.
CRM_MGRREP	ACTVT MGR_REPORT	Segmentation Basis Report	Reports are used for creating or updating the segmentation basis. This authorization object is used to check whether the user has the authorization to view, create, delete, and change reports for segmentation basis.
CRM_MKDSTP	ACTVT	Import/Export of Data Sources and Attribute Lists	This authorization object allows a user to import and export data sources or attribute lists. For example, through this authorization object, the user is authorized

Authorization Object	Field	Description	Usage
			to transport data from a consolidation system to a production system.

If the users are not assigned to any role or profile, they cannot process any segment objects.

For more information, see Customizing for:

- *Customer Relationship Management* › *Marketing* › *Segmentation* › *General Setting* › *Define Usages for Segments*
- *Customer Relationship Management* › *Marketing* › *Segmentation* › *Classic Segmentation* › *Define Reports for Creating Segmentation Basis*

Access Control Engine

To activate access restrictions on channel partner campaigns, especially in the WebClient UI, designated for the channel partner, the following rules must be activated in ACE:

Table 49

Rule	Right
MKT_TG_FOR_CPE	MKT_TG_FOR_CPE_CHANG
MKT_TG_FOR_CPE	MKT_TG_FOR_CPE_FULL
MKT_TG_FOR_CPE	MKT_TG_FOR_CPE_READ

Communication Channel Security

If required, authentication and encryption protocols such as SNC and SSL can be obtained from SAP Service Marketplace on SAP Service Marketplace at service.sap.com/securityguide. You can add these protocols to the SAP protocols DIAG and RFC as shown in the following table:

Table 50

Communication Path	Protocol Used	Type of Data Transferred
Server to server in an SAP system	SAP DIAG (SNC)	General data
Server to server across SAP systems	RFC (SNC)	General data
Internet	TCP/IP (SSL)	General data

Communication Destination

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section:

Table 51

Destination	Delivered?	Type	User Authorizations	Descriptions
SAP NetWeaver BW	No	RFC	User, password	Additional SAP system for data evaluation
SAP NetWeaver AS	Yes	DIAG	User, password	n.a

Data Storage Security

Data is stored in the SAP NetWeaver AS database table. Depending on the user, the appropriate rights, read, write, change, and delete, are required. Extra data storage security is not required.

Checklist

Table 52

Feature	Check	How to Check
Change a segmentation element or some of its properties.	User settings for the corresponding authorization object.	If we are not authorized to perform changes, the system rejects your changes.

For more information about internet security, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *SAP Web Dispatcher as a URL Filter*.

3.1.5 Mail Forms

Mail forms represent templates for personalized communications using the following channels: e-mail, fax, or SMS. The mail forms application is built on the SAP NetWeaver application server (SAP NetWeaver AS).

Security Aspects of Data, Data Flow and Processes

With the mail forms application, you can create personalized mailings. The application can send emails with personalized content derived from the master data as well as transactional data that is available in the system. To ensure the protection of such data, it is important that appropriate user authorizations are maintained for this application. For sending emails, faxes, and short messages, the application uses the infrastructure provided by SAP NetWeaver Application Server. The application relies on appropriate settings of that communication infrastructure.

User Administration and Authentication

User Management

Mail forms use the normal user management of SAP NetWeaver AS and require dialog users. Mail forms can be transported to other systems. This requires a remote function call (RFC) connection with a user and password. In Customizing, the RFC user can be set to the current dialog user instead of a default RFC user, allowing for individual authorizations.

Standard Users

Table 53

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Standard Roles

Table 54

Business Role	PFCG Role	Description
MARKETINGPRO	SAP_CRM_UIU_MKT_PROFESSIONAL	Marketing Professional

Standard Authorization Objects

Table 55

Authorization Object	Field	Value	Description
CRM_IM_ML	ACTVT	01 02 03 06	Create Change Display Delete
CRM_IM_ML	ACTVT	21	Transport of mail forms to other systems via RFC

Access Control Engine

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for mail forms in ACE Customizing because the rules that are delivered are dummy rules. For more information, see the Access Control Engine [page 324] section.

Communication Channel Security

The following table details the communication channels that the application uses, and the respective protocols, data types transferred, and data requiring special protection.

Table 56

Communication Channel	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Mail Server	SMTP	Multi-purpose internet mail extensions (MIME) e-mail	Personal data
Fax server	Dependent on SAP NetWeaver settings	Dependent on SAP NetWeaver settings	Personal data
Short messages server	Dependent on SAP NetWeaver settings	Dependent on SAP NetWeaver settings	Personal data
WWW	HTTP	Web pages	-
Digital Asset Management System	HTTP	URLs to assets	Digital Assets
SAP CRM system to SAP CRM system	RFC	Mail form	-

To protect RFC and DIAG connections, use Secure Network Communication (SNC) and to protect HTTP connections, use Secure Sockets Layer (SSL) protocol.

➡ Recommendation

We recommend using SSL and SNC whenever possible.

The purpose of this application is the creation of personalized mailings resulting in the use of personal data in related scenarios such as e-mail marketing campaigns. To ensure protection of such personal data, authorized users are required to adhere to standard legal requirements.

Network Security

For more information, see the section Network and Communication Security [page 29].

Communication Destinations

The following table details the communication destination used by the application:

Table 57

Destination	Delivered	Type	User Authorizations	Description
SAP CRM system	No	RFC	User password	SAP CRM system to which mail forms can be transported

Internet Communication Framework Security

Activate only those services required by the applications actually running in your system. Services required for mail forms are:

- CRM TRACKING
- CONTENTSERVER

To activate these services, use transaction `SICF`.

If your firewalls use URL filtering, note them and adjust your firewall settings accordingly. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* : Search for *Activating and Deactivating ICF Services*.

For more information about ICF security, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for Connectivity and Interoperability Technologies* › *RFC/ICF Security Guide* .

3.1.6 Campaign Management

Campaign management including campaign automation integrates several functions, such as key figure planning, e-mail, surveys, and multiple link tracking, to support marketing modeling and execution.

The functions listed above use SAP NetWeaver Application Server (SAP NetWeaver AS), SAP NetWeaver Business Warehouse (SAP NetWeaver BW), and SAP ERP.

Important Notes

Table 58

Title	SAP Note	Comment
Explicitly granting read permissions in java.policy	675851	Read permission for campaign automation applet
Version 2.6.2 of marketing calendar	1496974	Marketing calendar security message

Security Aspects of Data, Data Flow and Processes

For High Volume Marketing Execution or File Export Execution, data is stored on a network share on which the CRM back end uses parallel processing for fast execution. This results in the creation of multiple packages in the form of files. For further processing, such as processing by mailing tool, sending to a letter shop, these packages must be picked up sequentially.

In this case, it is important that only users with the proper authorizations can access this data since it can contain sensitive business partner information. You must also check that the tools that are processing this information meet all security requirements.

Finally the data must be deleted after usage. This is done in the follow-on processes and not in SAP CRM.

User Management and Authentication

Campaign management including campaign automation uses the normal user management of SAP NetWeaver AS and requires dialog users. If surveys are used, Internet users are also required.

Key figure planning involves online updates of data in SAP NetWeaver BW. This requires a remote function call (RFC) connection with a user and password. In Customizing, the RFC user can be set to the current dialog user instead of a default RFC user, allowing for individual authorizations.

In the Multichannel Foundation offer harmonization scenario, campaign information is transferred to SAP ERP. This also requires an RFC connection.

Standard Users

Table 59

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary
SAP NetWeaver BW	Normal user	No	Dialog user	Arbitrary
SAP ERP	Technical user	No	System user	Arbitrary

Standard Roles

Table 60

Business Role	PFCG Role	Description
`MARKETINGPRO`	`SAP_CRM_UIU_MKT_PROFESSIONAL`	`Marketing Professional`

Other Relates Roles

For collaborative campaign management scenario:

Table 61

Business Role	PFCG Role	Description
CHM-CM	SAP_CRM_UIU_CHM_CHANNELMANAGER	Channel Manager
CHM-PM	SAP_CRM_UIU_CHM_PARTNERMANAGER	Partner Manager

For loyalty Management Scenario

Table 62

Business Role	PFCG Role	Description
LOY_PRO	SAP_CRM_UIU_LOY_PROFESSIONAL	Loyalty Manager

For trade promotion management scenario:

Table 63

Business Role	PFCG Role	Description
TPM_PRO	SAP_CRM_UIU_TPM_PROFESSIONAL	TPM Professional

Role and Authorization Concept of Campaign Management

The standard role for Campaign Management is the Marketing Professional. With that all necessary authorizations are maintained to use the marketing functions required.

Note

For usage of Marketing Funds Management Integration, activate the business function CRM_MKT_FM first. To use Multichannel Foundation campaigns as part of offer harmonization, activate the business function CRM_MCF_R1 first.

Campaign Management is also used in the channel scenario for Collaborative Campaign Management. The roles Channel Manager and Partner Manager contain authorizations for campaign management usage but note that the Partner Manager role has restricted access only.

For the Partner Manager role, you need to maintain the ACE authorization.

Note

For usage of Collaborative Campaign Management, activate the business function CRM_MKT_CCM first.

Standard Authorization Objects

Several authorization objects allow for specific authorizations depending on the type of the marketing project involving the employee responsible as a central entity. These authorization objects are listed in the following table:

Table 64

Authorization Object	Description
CRM_CPG	CRM Marketing: Business Object Campaign
CRM_CPGAGR_CRM	CRM Marketing: Campaign Authorization Group
CRM_CPGASG	CRM Marketing: Campaign Assignments
CRM_CPGCTP	CRM Marketing: Campaign Type
CRM_CPGRES	CRM Marketing: Person Responsible for Campaign
CRM_CPGTPL	CRM Marketing: Campaign Template
CRM_MPLAGR	CRM Marketing: Marketing Plan Authorization Group
CRM_MPLRES	CRM Marketing: Person Responsible for Marketing Plan
CRM_MPL_AD	CRM Marketing: General Settings
CRM_MPT	CRM Marketing: Business Object Marketing Plan
CRM_FDT	Authorization Object – Rule Policy
CRM_ACT	Authorization Object CRM Order – Business Object Activity

For High Volume Marketing Execution or the File Export Execution of a channel partner campaign (collaborative campaign planning scenario), the following additional authorizations are required for a successful execution:

Table 65

Authorization Object	Authorization Fields
S_LOG_COM	COMMAND MKTDIRLIST, MKTDIR
S_DATASET	ACTVT: 33,34,A6, A7 FILENAME: * PROGRAM: CRM_MKTHV_EXE_BATCH, SAPLCRM_MKTHV_FPP_RFC

With this authorization, you enable the creation of subdirectories within the network file share that you configured for the high-volume marketing execution or the file export execution of a channel partner campaign (collaborative campaign planning scenario). For more information, see the Customizing documentation for high-volume marketing execution. Make sure that the access rights to this network share are appropriately restricted to avoid unauthorized access and manipulation of the data stored in this share.

To enable a user to navigate directly from a link in the campaign UI application, a third-party product (such as an http server, or an ftp server) is needed. Make sure that you limit access rights in the third-party product, in a way that only authorized users are able to use this service or access the files and directories. This is relevant mainly for the resulting files of a high-volume execution or file export execution of a channel partner campaign (collaborative campaign planning scenario).

With the following authorization, you enable the execution of RFC modules that contain significant parts of the high volume marketing execution implementation:

Table 66

Authorization Object	Authorization Fields
S_RFC	RFC_NAME CRM_MKTHV_FPP_RFC

For Marketing Funds Management Integration, the following additional authorizations for funds management related functionality are needed:

Table 67

Authorization Object	Authorization Fields
CRM_FM_FND	ACTVT: 45 (Allow)
CRM_FM_FPO	ACTVT: 01 (Create), 02 (Change), 03 (Display)
CRM_FM_FU	ACTVT: 01 (Create), 02 (Change), 03 (Display, 06 (Delete), C4 (Close Out)

For more information, see Funds Management [page 107].

For the SAP Real-Time Offer Management (SAP RTOM) software integration used in Web service CRM_MKT_RTOM_WS, the following additional authorization is needed:

Table 68

Authorization Object	Authorization Fields
S_RFC	RFC_NAME CRM_MKT_RTOM_SERVICE

For bounce management, the following additional authorization is needed:

Table 69

Authorization Object	Authorization Fields
S_RFC	RFC_NAME CRM_MKTHV_BOUNCE

In the offer harmonization scenario, the RFC user for the SAP CRM to SAP ERP transfer should be granted a profile that contains the following authorization objects and values:

Table 70

Authorization Object	Field 1	Value 1	Field 2	Value 2	Field 3	Value 3
S_RFC	RFC_TYPE	FUGR	RFC_NAME	CRM_CMP_PROMO	ACTVT	16
S_RFC	RFC_TYPE	FUGR	RFC_NAME	ERFC	ACTVT	16
S_RFC	RFC_TYPE	FUGR	RFC_NAME	ARFC	ACTVT	16

The RFC user also needs the following authorizations in SAP ERP:

Table 71

Authorization Object	Field 1	Value 1
`S_TCODE`	`TCD`	`WAK3`
`S_TCODE`	`TCD`	`WAK2`
`S_TCODE`	`TCD`	`WAK1`

Access Control Engine

For the access restrictions on channel partner campaigns, especially on a UI that is designated for the channel partner, you must ensure that the following rules in ACE are activated:

- `CPG_CCM_CHANGE`
- `CPG_CCM_DISPLAY`
- `CPG_CCM_CHANGE2`
- `CPG_CCM_DISPLAY2`

Communication Channel Security

A typical marketing activity, such as an e-mail campaign that must reach potential customers without hurdles and that contains no sensitive data, may not contain data requiring special protection. If necessary, you can implement the required protection.

If required, authentication and encryption protocols such as secure network communication (SNC) and secure sockets layer (SSL) can be obtained on SAP Service Marketplace at service.sap.com. You can add these protocols to the SAP protocols Dynamic Information and Action Gateway (DIAG) and remote function call (RFC), as shown in the following table:

Table 72

Communication Path	Protocol Used	Type of Data Transferred
Mail server	Simple Mail Transfer Protocol (SMTP)	Multipurpose Internet Mail Extensions (MIME) formatted
Server to server within an SAP system	SAP DIAG (SNC)	General data
Server to server across SAP systems	RFC (SNC)	General data
Internet	TCP/IP (SSL)	General data

Network Security

Observe the usual security standards for multiple link tracking, surveys, e-mail links, and so on. Accordingly, use a firewall with a demilitarized zone (DMZ), a reverse proxy server, and so on.

Similar to the *Authorization Objects* section above, be aware that some scenarios as high-volume executions or channel partner campaign executions might write files to a network share that are supposed to be accessible by the user via link in the campaign UI application.

Make sure that you limit access rights in the third-party product, in such a way so that only authorized users are able to use this service or access the files and directories. This is relevant mainly for the files resulting from a high-volume execution or file export execution of a channel partner campaign (collaborative campaign planning scenario).

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 73

Destination	Delivered?	Type	User, Authorizations	Descriptions
SAP NetWeaver BW	No	RFC	User, password	Additional SAP system for data evaluation
SAP NetWeaver AS	Yes	DIAG	User, password	N/A
SAP ERP	No	RFC	User, password The user in SAP ERP should be a system user. Other than the technical authority required to perform an RFC call and execute a program, no further authorization is required.	Used for communication with the SAP CRM server for data transfer and response messages in certain marketing scenarios. The RFC user is created by an SAP ERP system administrator.

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

For High Volume Marketing Execution, take into account the guidelines in the section, *Security Aspects of Data, Data Flow and Processes.*

Using Logical Path and File Names to Protect Access to the File System

In collaborative campaign management, data is saved in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by collaborative campaign management and for which programs these file names and paths apply:

Logical File Names Used in Collaborative Campaign Management

The logical file name `MARKETING_FILES` is used to validate physical file names.

The following programs use the logical file name `MARKETING_FILES`:

- `CRM_MKTTGGRP_EXPORT_BATCH`
- `SAPLCRM_MKTTGGRP_EXPORT` with function `CRM_MKTTGGRP_FE_WRITE_FILE`

The following file names are available:

1. *Logos for the Channel Partner*
2. *Signatures of Partner Contacts*
3. *Photos of Partners Contacts*

The file name is BP_ID+_+ Document type. The file extension is not changed.

Table 74

Document Type	Description	Used For
CHMLOGOS	Logo for e-mail (small size)	Corporate Channel Partner or Channel Partner
CHMLOGOL	Logo for letter (large size)	Corporate Channel Partner or Channel Partner
CHMSIGNATS	Signature for e-mail (small size)	Partner Contacts
CHMSIGNATL	Signature for letter (large size)	Partner Contacts
CHMPHOTOS	Photo for e-mail (small size)	Partner Contacts
CHMPHOTOL	Photo for letter (large size)	Partner Contacts

In addition, file name *CSV File* (Campaign ID+Timestampt.CSV) is available.

Logical Path Names Used in Collaborative Campaign Management

The logical file names listed above all use the logical file path MARKETING_FILES.

Structure

MARKETING_FILES (default path for marketing)

Collaborative Campaign (Logical system + Campaign ID

Partner Campaign 1 (Partner Campaign ID)

Partner Campaign n (Partner Campaign ID)

(For example, A0GCLNT000_WINTERCAMPAIGN2008/C_0001–719–6)

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physcial path using the transactions FILE (client-independent) and SF01 (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log. For more information, see the following references:

- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* : Search for *Logical File Names*
- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for the Application Server* › *Security Guides for the AS ABAP* › *SAP NetWeaver Application Server ABAP Security Guide* › *Special Topics* › *Protecting Access to the File System Using Logical Path and File Names*
- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* : Search for *Security Audit Log*

Checklist

Table 75

Feature	Check	How to Check
Change a marketing project or some of its properties	User settings for the corresponding authorization object	If you are not authorized to perform changes, the system rejects your changes.
Enter and save key figures for planning	Customizing for RFC destinations	If a dialog user has been maintained and you are not authorized to perform changes, the system rejects your changes.

For more information about Internet security, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *SAP Web Dispatcher as a URL Filter*.

3.1.7 Account Defaults

Why is Security Necessary?

Security in Account Defaults in the marketing area is necessary because account defaults are used to maintain sensitive data such as customer buying patterns, default dates, or account calendars for trade promotions or deals. Access to such data must be restricted.

User Administration and Authentication

User Management

Table 76

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal User	No	Dialog User	No	To be maintained by an SAP CRM system administrator

User Management Tools

Table 77

Tool	Description
User Maintenance (transaction `SU01`)	For more information, see User Administration and Authentication [page 18].

User Types

The personal user type is used, such as:

- Dialog Users
- Background Users

To use the standard processes that are delivered, customers must create individual users.

Authorization Objects

Account Defaults uses the SAP NetWeaver Application Server (SAP NetWeaver AS) authorization technique. The recommendations and guidelines for authorizations as described in the *SAP Netweaver Application Server ABAP Security Guide*also apply to this application.

The SAP NetWeaver AS authorization concept assigns authorizations to users based on roles. For role administration, use the profile generator (transaction `PFCG`) on SAP NetWeaver AS ABAP.

For the description of the authorization procedure used in SAP CRM master data processing, see Component-Specific Guidelines: SAP CRM [page 68].

The following authorization objects and authorization fields are used for Accounts Default maintenance:

Standard Authorization Objects

Table 78

Authorization Object	Description
`CRM_DEF`	`ACTVT`

Additional Authorization Checks

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for account defaults in ACE Customizing, because the rules in the SAP standard system are dummy rules.For more information, see the Access Control Engine [page 324] section.

Network and Communication Security

The network topology for marketing is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. For more information about this network topology, see Network and Communication Security [page 29].

Communication Channel Security

The following communication channels are used:

- Business document (BDoc) type (for data exchange with mobile client)
- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Table 79

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a web browser to SAP CRM server	HTTP/HTTPS	All application data	Passwords and all sensitive SAP CRM data

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

3.1.8 Deal Master

The deal master application allows you to maintain deals. A deal is a set of promotional constraints that are applied to a predefined set of customers for predefined products. A deal can be created and maintained both online and offline and is used as template for trade promotions. It integrates key figure planning and e-mail.

The deal master application uses SAP NetWeaver Application Server (SAP NetWeaver AS) and SAP NetWeaver Business Warehouse (SAP NetWeaver BW).

Security Aspects of Data, Data Flow and Processes

The communication between the WebClient UI/User and the SAP CRM back end is achieved for a dialog user with the assignment to the business role and the corresponding PFCG role, communication protocol HTTP/HTTPS.

The deal master uses the BW planning services. It uses the synchronous RFC to retrieve and save planning data.

Business Roles

Table 80

Business Roles	PFCG Role	Description
TPM_PRO	SAP_CRM_UIU_TPM_PROFESSIONAL	TPM Professional

User Management and Authentication

The deal master application uses the normal user management of the SAP NetWeaver AS and requires dialog users.

Key figure planning involves online updates of data in SAP NetWeaver BW. This requires a remote function call (RFC) connection with a user and password. In Customizing, the RFC user can be set to the current dialog user instead of a default RFC user, allowing for individual authorizations.

Users

Table 81

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary
SAP NetWeaver BW	Normal user	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations depending on the type of marketing project (deal or trade promotion) involving the employee responsible as a central entity. These authorization objects are listed in the following table:

Table 82

Authorization Object	Description
CRM_DLM	CRM Marketing: Business Object Deal
CRM_DLMAGR	CRM Marketing: Deal Authorization Group

Authorization Object	Description
`CRM_DLMCTP`	CRM Marketing: Campaign Type
`CRM_DLMRES`	CRM Marketing: Person Responsible for Deal
`CRM_TPM`	CRM Marketing: Business Object Trade
`CRM_TPMAGR`	CRM Marketing: Campaign Authorization Group
`CRM_TPMCTP`	CRM Marketing: Campaign Type
`CRM_TPMRES`	CRM Marketing: Person Responsible for Trade
`CRM_TPMVER`	CRM Marketing: Authorization Object for Viewing the Version Data

Session Security Protection

For more information, see Session Security Protection [page 29].

Network and Communication Security

Communication Channel Security

It is possible to conduct an e-mail campaign from a deal, although it is more common to use such marketing activity from other marketing projects such as campaigns or trade promotions. Such an e-mail campaign typically does not contain sensitive data; it reaches potential customers without hurdles and the data may not require special protection. If necessary, you can implement the required protection.

If required, the authentication and encryption protocols secure network communication (SNC) and secure sockets layer (SSL) can be obtained on SAP Service Marketplace at service.sap.com. You can add these protocols to the SAP protocols Dynamic Information and Action Gateway (DIAG) and remote function call (RFC), as shown in the following table:

Table 83

Communication Path	Protocol Used	Type of Data Transferred
Mail server	Simple Mail Transfer Protocol (SMTP)	Multipurpose Internet Mail Extensions (MIME) formatted
Server to server within an SAP system	SAP DIAG (SNC)	General data
Server to server across SAP systems	RFC (SNC)	General data
Internet	TCP/IP (SSL)	General data

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 84

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver BW	No	RFC	User, password	Additional SAP system for data evaluation
SAP NetWeaver AS	Yes	DIAG	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

Checklist

Table 85

Feature	Check	How to Check
Change a deal or some of its properties	User settings for the deal authorization objects	If you are not authorized to perform changes, the system rejects your changes.
Generate a trade promotion from a deal	User settings for the deal and trade promotion authorization objects	The system only generates a trade promotion if you have the necessary authorization.
Enter and save key figures for planning	Customizing for RFC destinations	If a dialog user has been maintained and you are not authorized to perform changes, the system rejects your changes.

3.1.9 Claims Management

Claims management is an application based on SAP Customer Relationship Management (SAP CRM) that enables you to capture and validate trade-related claims and payments

Added value of claims management include the following:

- Full support of financial execution of trade promotions in SAP CRM, as compared to processing that is split between the front end and the back end
- Central repository of claims (invoices, deductions, scheduled payments, and so on)
- Form-based claim validation
- Full deduction management capabilities
- Chargeback and write-off processing
- Full integration into funds management
- Full integration into trade promotion management
- Full integration into SAP ERP Financials and SAP Dispute Management

Security Aspects of Data, Data Flow and Processes

The following sequence diagrams describe the process of transferring a Dispute Case to SAP CRM for further processing and the deduction processing including settlement in SAP CRM and the creation of a credit memo in SAP ERP.

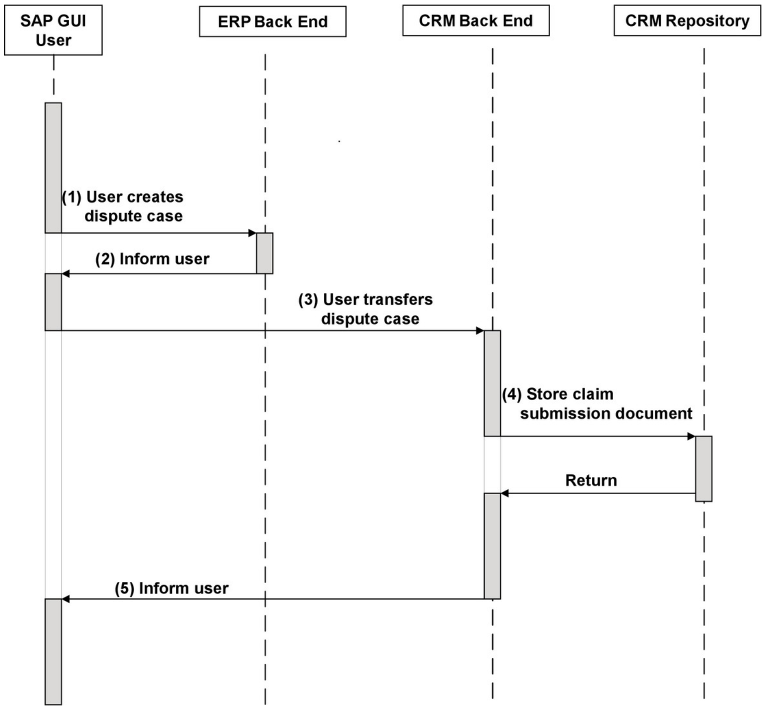

SAP GUI User
ERP Back End
CRM Back End
CRM Repository
(1) User creates dispute case
(2) Inform user
(3) User transfers dispute case
(4) Store claim submission document
Return
(5) Inform user

Figure 6: Overview of Process Steps for Transferring a Dispute Case to SAP CRM

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

Table 86

Step	Description	Security Measure
1	User creates dispute case	Dialog user with restricted access to system. SQL to connect to DB
2	ERP back-end system informs user	Not applicable
3	User transfers dispute case	Dialog user with restricted access to system Conversion of data in XML format Use of RFC and BDoc to transfer data
4	Store claim submission document	SQL to connect to DB
5	Inform user	Not applicable

The figure below shows an overview of the deduction processing.

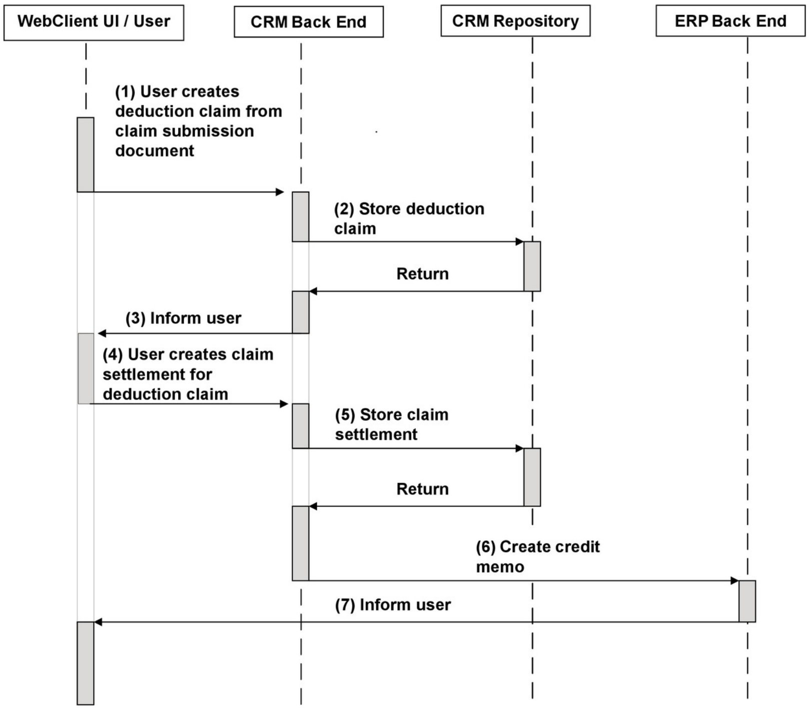

WebClient UI / User
CRM Back End
CRM Repository
ERP Back End
(1) User creates deduction claim from claim submission document
(2) Store deduction claim
Return
(3) Inform user
(4) User creates claim settlement for deduction claim
(5) Store claim settlement
Return
(6) Create credit memo
(7) Inform user

Figure 7: Overview of Process Steps for Deduction Processing (Including Settlement in SAP CRM and Creation of Credit Memo in SAP ERP)

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

Table 87

Step	Description	Security Measure
1	User creates deduction claim from claim submission document	User Type: Dialog user with assignment to business role and PFCG role, communication protocol HTTP/HTTPS
2	Store deduction claim	SQL to connect to DB
3	Inform user	Not applicable
4	User creates claim settlement for deduction claim	User Type: Dialog user with assignment to business role and PFCG role, communication protocol HTTP/HTTPS
5	Store claim settlement	SQL to connect to DB
6	Create credit memo	Use of BDoc and RFC
7	Inform user	Not applicable

User Administration and Authentication

User Management

Table 88

System	User	Delivered?	Type	Default Password	Description
SAP CRM	Personal user	No	Dialog user	No	Mandatory user who can access claims management transactions. To be maintained by an SAP CRM system administrator.
SAP NetWeaver Business Warehouse (SAP NetWeaver BW)	Personal user	No	Dialog user	No	Mandatory user who can access SAP NetWeaver BW applications. To be maintained by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user who can process background tasks. To be maintained by an SAP CRM system administrator.
SAP ERP	Personal or technical user	No	Dialog or system user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, user can be a personal user or a system RFC user. To be maintained by an SAP ERP system administrator.

User Management Tools

Table 89

Tool	Description
User Maintenance (transaction `SU01`)	For more information, see User Administration and Authentication [page 18].

User Types

The personal user type is used to create users such as the following:

- Dialog users
- Background users

Customers must create the following users:

- Individual users to use the standard processes that are delivered in the standard system
- Initial identification parameters, such as the password and certificate for the users

Authorizations

Claims management uses the authorization technique provided by SAP NetWeaver Application Server (SAP NetWeaver AS). Therefore, the recommendations and guidelines for authorizations as described in *SAP NetWeaver Application Server ABAP Security Guide* also apply to the application.

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

The following authorization objects and authorization fields are used:

Table 90

Authorization Object	Authorization Fields
CRM_CL_CSD (Business object claim submission document)	ACTVT
CRM_CL_CSR (Business object claim settlement request)	ACTVT
CRM_CL_CPP (Business object claim prepayment)	ACTVT
CRM_CL_CCB (Business object chargeback)	ACTVT
CRM_CL_RES (Business object chargeback)	ACTVT
CRM_ORD_LP (Visibility in organization model)	CHECK_LEV (Scope of processed objects) PR_TYPE (Transaction type) ACTVT
CRM_ORD_OE (Allowed organizational units)	SALES_ORG (Sales organization) SERVICE_OR (Service organization) DIS_CHANNE (Distribution channel) SALES_OFFI (Sales office) SALES_GROU (Sales group) ACTVT
CRM_ORD_OP (Own documents)	PARTN_FCT (Partner function) PARTN_FCTT (Partner function category) ACTVT
CRM_ORD_PR (Business transaction type)	PR_TYPE (Transaction type) ACTVT
CRM_CL_TDF (Tax Difference Report authorization object)	ACTVT
CRM_CLA_EX (Claim expiration authorization object, for the UI and the closing report, CRMD_CLA_CLOSE)	ACTVT
CRM_CL_SFA (Search for settled agreements, in case of claims that validate enhanced rebates trade promotions)	ACTVT

Network and Communication Security

The network topology for claims management is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and the corresponding section of Component-Specific Guidelines: SAP CRM [page 68] also apply to trade claims management.

For more information, see Network and Communication Security [page 29].

Communication Channel Security

The following communication channels are used:

- Remote function call (RFC)
- Business document (BDoc) type: `BUS_TRANS_MSG`
- ABAP Structured Query Language (SQL) for the connection to the database

Communication Destinations

Table 91

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, conditions
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, conditions
CRM server to ERP server	RFC	System ID, client, and host name, all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client, and host name, all application data	System information and ERP data
CRM server to BI server	RFC	System ID, client, and host name, all application data	System information and CRM data
CRM server to Internet Pricing and Configurator (IPC)	RFC	Pricing conditions	System information and CRM data
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data
SAP CRM to SAP Supply Chain Management (SAP SCM) – SAP Advanced Planning & Optimization (SAP APO)	RFC	Application data	Password and user for SAP SCM – SAP APO required
SAP CRM to SAP ERP Financials	RFC	Application data (Posting claim submission data)	System Information and CRM data

In claims submissions, the transaction launcher is also used to connect to the SAP ERP system in the Web UI to view posted claim submission data.

3.1.10 Trade Promotions

Trade promotion management allows you to maintain trade promotions. A trade promotion can be created and maintained and is used to plan promoted sales for a planning account. It integrates key figure planning.

Trade promotion management uses SAP NetWeaver Application Server (SAP NetWeaver AS) ,SAP NetWeaver Business Warehouse (SAP NetWeaver BW), and SAP ERP.

Security Aspects of Data, Data Flow and Processes

The figure below shows an overview of the data flow for Trade Promotions.

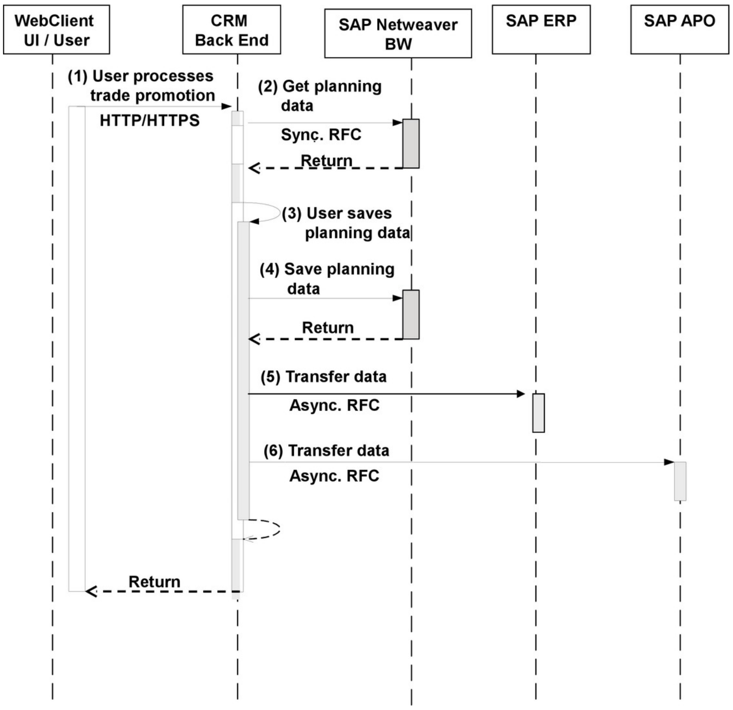


Figure 8: Overview of Process Steps for Trade Promotions

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

Table 92

Step	Description	Security Measure
1	User processes trade promotion	User Type: Dialog user with assignment to business role (for example `TPM_PRO`) and corresponding PFCG role, communication protocol, HTTP/ HTTPS.
2	Get planning data	Not applicable (synchronous RFC)
3	User saves planning data in SAP CRM	Not applicable
4	Save planning data	Not applicable (synchronous RFC)
5	Transfer data to SAP ERP	Not applicable (synchronous RFC)

Step	Description	Security Measure
6	Transfer data to SAP APO	Not applicable (synchronous RFC)

Business Roles

Table 93

Business Role	PFCG Role	Description
TPM_PRO	SAP_CRM_UIU_TPM_PROFESSIONAL	TPM Professional
TRD_CLM_PRO	SAP_CRM_UIU_TCM_PROFESSIONAL	Trade Claims Professional
TRD_FIN_PRO	SAP_CRM_UIU_TFM_PROFESSIONAL	Trade Finance Professional
SPL	SAP_CRM_UIU_SPL_PROFESSIONAL	PFCG Role for Service Parts Logistics Management Professional

User Management and Authentication

Trade promotion management uses the normal user management of SAP NetWeaver and requires dialog users.

Key figure planning involves online data updates in SAP NetWeaver BW and SAP ERP. This requires a remote function call (RFC) connection with a user and password. In Customizing, the RFC user can be set to the current dialog user instead of a default RFC user, allowing for individual authorizations.

Users

Table 94

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary
SAP NetWeaver BW	Normal user	No	Dialog user	Arbitrary
SAP ERP	Normal user	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 95

Authorization Object	Field	Value	Description

CRM_TPM	*ACTVT*	01(Create or generate)
		02(Change)
		03(Display)
		06(Delete)
			CRM Marketing: Business Object Trade. Alphanumeric code that describes activities.

Authorization Object	Field	Value	Description

		45(Allow)
		72(Plan)	

CRM_TPMAGR	*ACTVT*	01(Create or generate)
		02(Change)
		03(Display)
		06(Delete)
		45(Allow)
		72(Plan)
			CRM Marketing: Campaign Authorization Group. Alphanumeric code that describes activities.

CRM_TPMAGR	*MKTPL_AUGR*	Authorization Group to be set by the customer	Stipulates which group of persons can access a trade promotion

CRM_TPMCTP	*ACTVT*	01(Create or generate)
		02(Change)
		03(Display)
		06(Delete)
		45(Allow)
		72(Plan)
			CRM Marketing: Campaign Type. Alphanumeric code that describes activities

CRM_TPMCTP	MKTPL_CPTY	Promotion type to be set by Customer	Identifies the type of a trade promotion

CRM_TPMRES	*ACTVT*	01(Create or generate)
		02(Change)
		03(Display)
		06(Delete)
		45(Allow)
		72(Plan)
			CRM Marketing: Person Responsible for Trade

CRM_TPMRES	*MKTPL_RESP*	Person responsible to be set by the customer	Key identifying a business partner in the SAP system
CRM_TPMVER	*ACTVT*	03(Display)	CRM Marketing: Authority Object for Viewing the Version Data

CRM_DEF	*ACTVT*	01(Create or generate)
		02(Change)
		03(Display)
		06(Delete)
			CRM Marketing: Account Defaults

Session Security Protection

For more information on the applicable session security measures, see Session Security Protection [page 29]

Network and Communication Security

Communication Channel Security

For information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 96

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP (Secure sockets layer (SSL))	General data

Network Security

For information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 97

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver BW	No	RFC	User, password. The user in SAP NetWeaver BW should be a system user. Besides the technical authority to do an RFC call and to execute a program, no further authorization is required. At a minimum, it should be able to call the following RFC function group: RSCRM_IMP_RFC_FACADE	Additional SAP system for data evaluation. Mandatory user for communication with CRM server when dealing with planning. Created by an SAP NetWeaver BW system administrator.
SAP ERP	No	RFC	The user in SAP ERP should be a system user. Besides the technical authority to do an RFC call and to execute a program, no further authorization is needed.	Mandatory user for communication with CRM server for response messages from SAP ERP. Created by an SAP ERP system administrator.
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

Checklist

Table 98

Feature	Check	How to Check
Change a trade promotion or some of its properties	User settings for the trade promotion authorization objects	You can only make changes if you have the proper authorization.
Display or change agreements associated with a trade promotion	User settings for the trade promotion and agreement authorization objects	You can only display or change the agreements if you have the proper authorization.
Enter and save key figures for planning	Customizing for RFC destinations	If a dialog user has been maintained, you can only make changes if you have the proper authorization.

3.1.11 Trade Promotion Guidelines

Trade promotion guidelines allow you to maintain guidelines for trade promotions. The system checks trade promotions against these guidelines when they are saved or when the status is changed.

Trade promotion guidelines use SAP NetWeaver Application Server (SAP NetWeaver AS).

Security Aspects of Data, Data Flow and Processes

Trade promotion guidelines is a CRM standalone application. It does not transfer data from SAP CRM to other SAP systems.

For dialog users the communication between the WebClient UI and the SAP CRM back-end is established with the assignment to a business role and the corresponding PFCG role, communication protocol HTTP/HTTPS.

Business Roles

Table 99

Business Role	PFCG Role	Description
`TPM_PRO`	`SAP_CRM_UIU_TPM_PROFESSIONAL`	TPM Professional

User Management and Authentication

Trade promotion guidelines use the normal user management of SAP NetWeaver AS and require dialog users.

Users

Table 100

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal use	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 101

Authorization Object	Description
`CRM_PPG`	CRM Marketing: Authorization Object Required to Use Promotion Guidelines
`CRM_PPGAUG`	CRM Marketing: Promotion Guideline Authorization Group

Session Security Protection

For more information on the applicable session security protection, see Session Security Protection [page 29].

Network and Communication Security

Communication Channel Security

For information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 102

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP (Secure Sockets Layer (SSL))	General data

Network Security

For information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 103

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

Checklist

Table 104

Feature	Check	How to Check
View or maintain a trade promotion guideline	User settings for the pricing guidelines for authorization objects	If you are not authorized to perform changes, the system rejects your changes.

3.1.12 Live Rates

Live Rates is a pay-for-performance concept for allocating budget for promotional spending. It has been designed for Trade Promotion Management. Like Trade Promotion Management, Live Rates also uses SAP Netweaver BW system for planning data.

> Note
>
> These guidelines apply in addition to the Trade Promotions Guidelines [page 102].

Security Aspects of Data, Data Flow and Processes

Live Rates uses the SAP NetWeaver BW planning services. It uses synchronous RFC to retrieve and save planning data.

For dialog users the communication between the WebClient UI and the SAP CRM back-end is established with the assignment to a business role and the corresponding PFCG role, communication protocol HTTP/HTTPS. Live Rates uses synchronous RFC data to retrieve and save planning data.

Business Roles

Table 105

Business Role	PFCG Role	Description
TRD_FIN_PRO	SAP_CRM_UIU_TFM_PROFESSIONAL	Trade Finance Professional

Authorization Objects

The system checks Live Rates against these guidelines when the Live Rates batch jobs are created, or when changing a Live Rates plan or an element.

Table 106

Authorization Object	Field	Value	Description
CRM_FMLRTP	*ACTVT*	45 (Allow)	Gives the user authorization to run live rates background jobs
CRM_LR_ELM	*ACTVT*	02 (Change) 03 (Display) 72 (Plan)	Alphanumeric code that describes activities

CRM_LR_ELM	*ACTVT*	02(Change)
		03(Display)
			Alphanumeric code that describes activities

Authorization Object	Field	Value	Description
		06(Delete	

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

Checklist

Table 107

Feature	Check	How To Check
Create or execute batch jobs for Live Rates	User settings for the Live Rates batch jobs authorization objects.	You can only create or execute batch jobs if you have the proper authorization.
Change a Live Rates Plan or Element	User settings for the Live Rates Plan or Element authorization objects as listed above.	You can only make changes if you have the proper authorization.
Enter and save key figures for planning Customizing for RFC destinations	If a dialog user has been maintained.	You can only make changes if you have the proper authorization.

3.1.13 Agreements

Trade promotion agreements provide the contractual framework for all events and activities that a key account manager generates with a customer for a given year. These agreement documents are nonbinding, but they provide a guideline for planning promotions.

Agreements use SAP NetWeaver Application Server (SAP NetWeaver AS).

Security Aspects of Data, Data Flow and Processes

For dialog users the communication between the WebClient UI and the SAP CRM back-end is established with the assignment to a business role and the corresponding PFCG role, communication protocol HTTP/HTTPS.

BI reports may be executed within an agreement under user request. Synchronous RFC is used to retrieve data from a BI report.

Business Roles

Table 108

Business Role	PFCG Role	Description
TPM_PRO	SAP_CRM_UIU_TPM_PROFESSIONAL	TPM Professional

User Management and Authentication

Agreements use the normal user management of SAP NetWeaver AS, and require dialog users.

Users

Table 109

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 110

Authorization Object	Description
CRM_TPM	SAP CRM Marketing: Business Object Trade
CRM_TPMAGR	SAP CRM Marketing: Campaign Authorization Group
CRM_TPMCTP	SAP CRM Marketing: Campaign Type
CRM_TPMRES	SAP CRM Marketing: Person Responsible for Trade
CRM_AGR	SAP CRM Marketing: Business Object Agreement
CRM_AGRAGR	SAP CRM Marketing: Agreements Authorization Group
CRM_AGRRES	SAP CRM Marketing: Person Responsible for Agreement

Session Security Protection

For more information on the applicable session security protection, see Session Security Protection [page 29].

Network and Communication Security

Communication Channel Security

For information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 111

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP (Secure sockets layer (SSL))	General data

Network Security

For information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 112

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

Checklist

Table 113

Feature	Check	How to Check
View or maintain an agreement	User settings for the agreement authorization objects	You can only make changes if you have the proper authorization.
Attach a trade promotion to an agreement	User settings for the trade promotion and agreement authorization objects	You can only attach a trade promotion to an agreement if you have the proper authorization.

3.1.14 Funds Management

Funds management is an application that allows brand owners to manage the distribution, consumption, and administration of funds. It provides one of the basic building blocks for market development funds (MDF) and trade promotion management (TPM). Funds management enables brand owners to track the status of the money in funds from the time it is budgeted through to the time it is paid out to the corresponding partners and customers. Funds management is integrated with SAP NetWeaver Business Warehouse (SAP NetWeaver BW) and SAP ERP.

The following functions are available:

- Funds plans and funds
- Fund usages
- Fund postings
- Budget postings
- Accruals
- Budget expiration
- Batch processing workbench
- Funds analytics
- Live rates funding

Security Aspects of Data, Data Flow and Processes

Funds Management is a standard SAP CRM application based on the business transaction for storing and manipulating data in the back-end and the Interaction Center WebClient UI Framework on the front-end. Consequently funds management reuses these framework security features related to data, and the data flow.

User Management and Authentication

Funds management uses the user management and authentication mechanisms of SAP NetWeaver; in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 funds management.

Standard Roles

Table 114

Business Role	PFCG Role	Description
TRD_FIN_PRO	SAP_CRM_UIU_TFM_PROFESSIONAL	Trade Finance Professional

Other Related Roles

For trade promotion management scenario:

Table 115

Business Role	PFCG Role	Description
TPM_PRO	SAP_CRM_UIU_TPM_PROFESSIONAL	TPM Professional

For collaborative campaign management scenario:

Table 116

Business Role	PFCG Role	Description
CHM_CM	SAP_CRM_UIU_CHM_CHANNELMANAGER	Channel Manager
CHM_PM	SAP_CRM_UIU_CHM_PARTNERMANAGER	Partner Manager

User Management

Table 117

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (SU01) transaction and the profile generator (PFCG) transaction.	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for funds management:

Table 118

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	End user	No	Dialog user	No	Mandatory user who can access funds management Customizing and funds management applications.

System	User	Delivered?	Type	Default Password	Description
					Created by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user who can process background jobs. Created by an SAP CRM system administrator.
SAP ERP	Technical user	No	System user	No	Mandatory user for data exchange between SAP CRM and SAP ERP. This user is only used with a remote function call (RFC) destination user. Created by an SAP ERP system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user for communication with the ERP server for response messages from SAP ERP. Created by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	The same RFC destination is used to communicate from SAP NetWeaver BW as for the other SAP CRM business objects. The user in the SAP CRM system who handles the requests from SAP NetWeaver BW to transfer data (user ALEREMOTE) needs to have two specific authorization objects: `CRM_ORD_LP` and `S_USER_GRP`. It is part of SAP NetWeaver BW authorization management to enforce proper authorization for SAP NetWeaver BW data so that users only see data for which they are authorized. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Business Warehouse*.

Authorizations

SAP GUI and WebClient UI authorizations, roles, and profiles are used. Furthermore, authorization objects that are created using *Maintain the Authorization Objects* (transaction SU21) are introduced.

Funds management has the following authorization:

Table 119

Authorization Object	Description
CRM_FM_FND	Authorization Object for Funds in Funds Management
CRM_FM_FNP	Authorization Object for Funds Plans in Funds Management
CRM_FM_ACL	CRM Funds Management: Authorization Object for Accruals
CRM_FM_BPO	Authorization Object for Budget Postings in Funds Management
CRM_FM_FPO	Authorization Object for Fund Postings in Funds Management
CRM_FM_FU	Fund Usage
CRM_FMLRTP	Authorization Object: CRM Live Rates Background Jobs

For the fund usage object, if the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for fund usage in ACE Customizing, because the rules that are delivered are dummy rules. For more information, see the Access Control Engine [page 324] section.

Authorization proposals are available in the standard system for the authorization objects mentioned above, as well as for the other authorization objects that are involved in funds management processes. For information, see the *Maintain the Assignments of Authorization Objects* (SU22) transaction. Use the CRM*FM* package for all possible types of applications for this purpose.

For more information about these authorization objects, see the *Maintain the Authorization Objects* (SU22) transaction and double-click the authorization object.

Communication Channel Security

The following communication channels are used:

- RFC
- BDoc type: BUS_TRANS_MSG
- ABAP SQL for the connection to the database

Network Security

The network for Funds Management is based on the SAP NetWeaver platform and middleware in SAP CRM. Therefore the security guidelines and recommendations described in the SAP *NetWeaver Security Guide* and the corresponding section of the Component-Specific Guidelines: SAP CRM [page 68] also apply to Funds Management. For more information, see Network and Communication Security [page 29].

Communication Destinations

The destination below is available in addition to the communication destination with the WebClient UI:

Table 120

Destination	Delivered?	Type	User, Authorizations	Description
SAP ERP	No	RFC connection	The user in SAP ERP should be a system user. Besides the technical authority to do an RFC call and to execute a program, no further authorization is needed. This might change in the future. For more information about how to proceed in this case, see SAP Note 926726.	Mandatory user for communication with CRM server for response messages from SAP ERP. Created by an SAP ERP system administrator

3.1.15 Loyalty Management

Why Is Security Necessary?

Security is necessary for the following reasons:

- The loyalty management component manages all of the data related to loyalty processes. This data can include personal data.
- Loyalty professionals and the interaction center agents (IC agents) in the loyalty area access SAP CRM data, such as customer master data or loyalty process-related data. It is crucial to protect customer-sensitive data.

Security Aspects of Data Flow and Processes

Loyalty Management data flow uses the IC WebClient to communicate with the SAP CRM back-end.

User Administration and Authentication

User Management

Table 121

Tool	Description
User Maintenance (SU01) transaction	For more information, see User Administration and Authentication [page 18].
The profile generator (PFCG) transaction	You use the profile generator transaction to create roles and assign authorizations to users in ABAP-based systems.

There are no users delivered in the standard system, so you must create individual users who can access all capabilities in the loyalty management application for use in the WebClient UI.

The standard tools are employed for user administration.

Users

Table 122

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user created using the *User Maintenance* (`SU01`) transaction	No	Created by an SAP CRM system administrator for accessing loyalty management
SAP CRM	Customizing user	No	Dialog user created using the *User Maintenance* (`SU01`) transaction	No	Created by an SAP CRM system administrator for customizing loyalty management
SAP CRM	Customizing user	No	Dialog user created using the *User Maintenance* (`SU01`) transaction	No	Created by an SAP CRM system administrator for customizing loyalty management

➜ Recommendation

Users created with a default password must change their password before first use.

Data Synchronization

The business partner object and its basic address information is replicated to a member object in loyalty management. This is a one-way synchronization, therefore no changes are made to the member object. Changes can only be made to the business partner. Changes are always replicated from business partner to member data.

Authorizations

The loyalty management scenarios use the SAP CRM standard for authorizations.

ABAP Stack Standard Roles Used by Loyalty Management in SAP CRM

Table 123

Role	Description
`SAP_CRM_UIU_LOY_PROFESSIONAL`	PFCG Role for Loyalty Professional using the CRM Web Client UI
`SAP_CRM_UIU_LOY_IC_AGENT`	PFCG Role for Loyalty IC Agent using the IC UI
`SAP_CRM_ECO_ISA_TU_B2C_LOYALTY`	Authorization for loyalty management anonymous user
`SAP_CRM_ECO_ISA_WU_B2C_LOYALTY`	Authorization for loyalty management user

If SAP NetWeaver Portal is used to access IC functions, make sure that you match roles between SAP NetWeaver Portal and the CRM server.

A user with the PFCG role `SAP_CRM_UIU_LOY_PROFESSIONAL` has access to the following rights:

Table 124

Object	Create	Modify	Delete	Read
Loyalty programs	X	X	X	X
Reward rule groups	X	X	X	X
Reward rules	X	X	X	X
Membership	X	X	X	X
Membership activity	X	X	X	X
Point accounts	X	X	X	X
Rule policies	X	X	X	X
Sales orders	X	X	X	X
Business partners	X	X	-	X
Partnership	X	X	X	X
Partner point account	X	X	X	X
Benefits	X	X	X	X
Complaints	X	X	X	X
Cards	X	X	X	X
Vouchers	X	X	X	X
Anonymous temporary cards	X	-	X	X
Organization membership	X	X	X	X

A user with the PFCG role `SAP_CRM_UIU_LOY_IC_AGENT` has access to the following rights:

Table 125

Object	Create	Modify	Delete	Read
Loyalty campaigns	-	-	-	X
Membership	X	X	X	X
Membership activity	X	X	X	X
Point accounts	-	-	-	X
Sales orders	X	X	X	X
Business partners	X	X	-	X

Standard Authorization Objects

The following table shows the security-relevant authorization objects used in the loyalty management scenarios:

Table 126

Authorization Object	Field	Value	Description
BSP_APPL	BSP_APPL BSP_VIEW	SPACE	This authorization object is for protecting a UI application. For a user to access a UI application through the transaction launcher, the user must have authorization to access the UI application.
CRM_FDT	ACTVT BRFP_APPL	01, 02, 03, 06, 21	This authorization object is for controlling the processes in the rule policy object.
LOY_MSH	ACTVT LOY_EVENT	01, 02, 03, 06	This authorization object is for controlling the processes in the membership object.
LOY_MEM	ACTVT	01, 02, 03, 06	This authorization object is for controlling the processes in the member object.
LOY_MA	ACTVT LOY_EVENT	01, 02, 03, 06 PR (Process), SI (Simulate)	This authorization object is for controlling the processes in the membership activity object.
LOY_PT_ACT	ACTVT LOY_EVENT	01, 02, 03, 06	This authorization object is for controlling the processes in the point account object.
CRM_LOY	ACTVT	01, 02, 03, 06	This authorization object is for controlling the processes in the loyalty program object.
CRM_CPG	ACTVT	01, 02, 03, 06, 45, 72	This authorization object is for controlling the processes in the loyalty program campaign creation.
CRM_RRG	ACTVT	01, 02, 03, 06	This authorization object is for controlling the processes in the reward rule group object.
CRM_RRL	ACTVT	01, 02, 03, 06	This authorization object is for controlling the processes in the reward rule object.
LOY_ATC	ACTVT	01, 02, 03	This authorization object is for controlling the processes

Authorization Object	Field	Value	Description
			in the anonymous temporary cards object.
`LOY_PPA`	`ACTVT` `LOY_EVENT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the loyalty partnership point account object.
`LOY_PSH`	`ACTVT` `LOY_EVENT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the loyalty partnership object.
`LOY_BNFT`	`ACTVT` `LOY_EVENT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the loyalty benefit object.
`LOY_BNGR`	`ACTVT` `LOY_EVENT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the loyalty benefit group object.
`LOY_MEM`	`ACTVT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the loyalty member object.
`LOYMSHBNFT`	`ACTVT` `LOY_EVENT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the loyalty membership benefit object.
`LOYAGRBNFT`	`ACTVT` `LOY_EVENT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in the account membership agreement benefit object.
`LOY_PTIER`	`ACTVT`	`01, 02, 03, 06`	This authorization object is for controlling the processes in loyalty partner tier mapping.

`CRM_LOYAGR`	`ACTVT`
	`MKTPL_AUGR`
		`01, 02, 03, 06`
		`45 - Allow`
		`72 - Plan`
			This authorization object is for controlling the processes in the loyalty program.

`CRM_CPGVOU`	`ACTVT`	`01, 02, 03`	This authorization object is for controlling the processes in the voucher object.

Loyalty Management for Partner and Channel Manager Roles Controlled with Authorizations

The standard mechanism of authorization checks is used for allowed transactions for a given role or user. The authorization objects for a user with channel and partner manager role are: `CRM_LOY`, `CRM_LOYAGR`, `CRM_LOYRES`, LOY_BNFT, LOY_BNGR, LOY_MA, LOY_MSH, LOY_PPA, LOY_PSH, and LOY_PT_ACT. For more information about settings, see the system documentation for the objects.

Access Control Engine

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for members, membership, member activity, point accounts, partnership, and partner point accounts in ACE Customizing, because the rules in the SAP standard system are dummy rules. For more information, see Access Control Engine [page 324].

Network and Communication Security

The network topology for Loyalty Management uses the IC WebClient in SAP CRM on the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in SAP CRM Powered by NetWeaver [page 301] also apply to the Loyalty Management.

Internet Communication Framework Security

Loyalty Management uses the Internet Communication Framework (ICF) services of the IC WebClient in SAP CRM. Therefore the security guidelines that apply to the IC WebClient also apply to Loyalty Management.

3.1.16 Digital Asset Management

You can use Digital Asset Management (DAM) as the central repository for your digital assets, such as photos, videos, or text documents.

Technical System Landscape

Digital asset management uses the following components and systems:

- SAP NetWeaver
- SAP NetWeaver Portal
- SAP CRM backend system
- SAP CRM content server
- TREX search engine

Optionally, you can use a graphics server, such as the Internet Graphics Service.

The following figure shows an overview of the system landscape for DAM and is followed by an explanation:

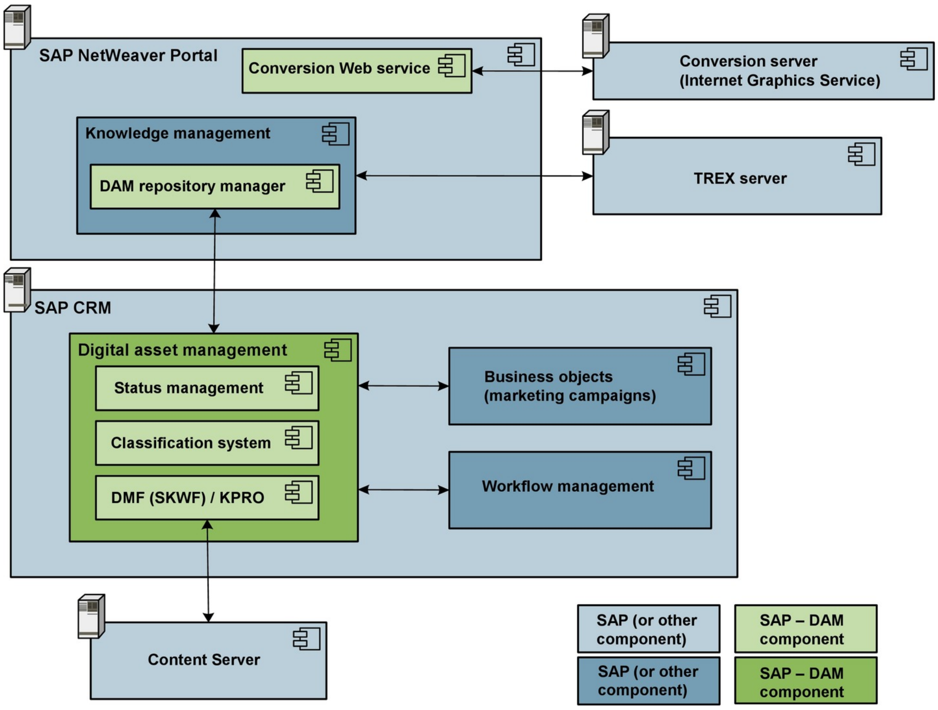


Figure 9: Technical System Landscape for Digital Asset Management

DAM in SAP CRM exchanges data with the following components:

- Workflow management
- Selected business objects, such as marketing campaigns
- Content server for SAP CRM

In SAP NetWeaver Portal, the following components exchange data:

- The DAM repository manager in Knowledge Management exchanges data with DAM in SAP CRM.
- The Knowledge Management component exchanges data with the TREX server.
- The DAM conversion web service exchanges data with the external conversion server, for example the Internet Graphics Service.

Security Aspects of Data, Data Flow and Processes

The data flow in digital asset management varies depending on the process that is used (for example, data upload, data download, or data search). For more information about the data transfer from the SAP CRM system to other SAP systems, such as the SAP NetWeaver Portal or the SAP content server, see the *Communication Channel Security* subsection.

The following figure shows the data flow for uploading digital assets, as an example for the data flow in digital asset management:

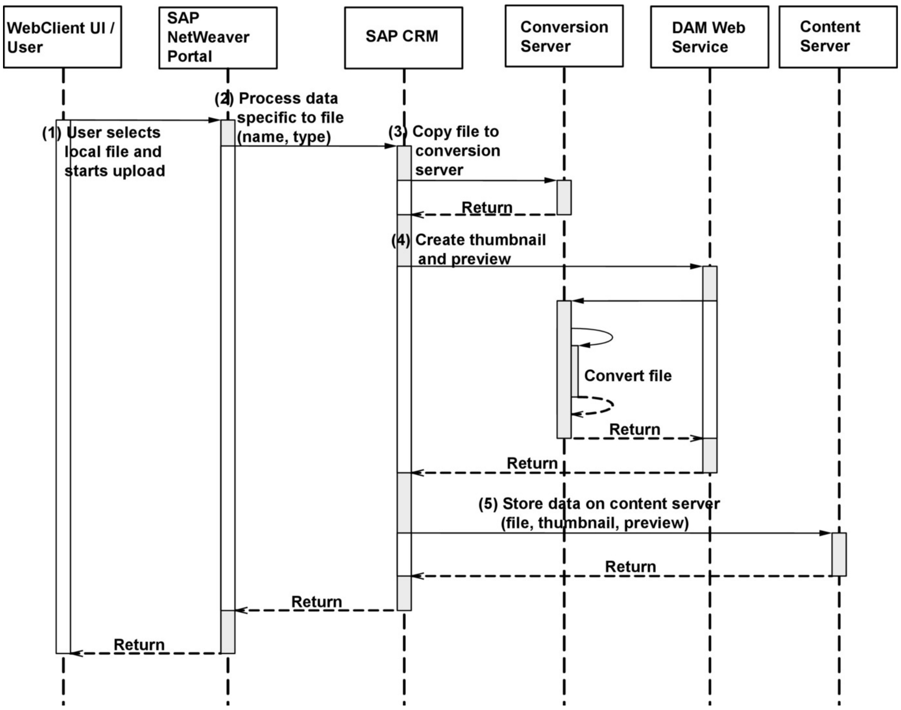

WebClient UI / User
SAP NetWeaver Portal
SAP CRM
Conversion Server
DAM Web Service
Content Server
(1) User selects local file and starts upload
(2) Process data specific to file (name, type)
(3) Copy file to conversion server
Return
(4) Create thumbnail and preview
Convert file
Return
Return
(5) Store data on content server (file, thumbnail, preview)
Return
Return
Return

Figure 10: Overview of Process Steps for Digital Asset Management

Table 127

Ste p	Description	Security Measure
1	User selects local file and starts upload	• Dialog user with assignment to NetWeaver Portal role and PFCG role • Communication protocol HTTP or HTTPS
2	Process data specific to file (name, type)	• Authorization check and check whether the MIME type is allowed • Virus scan (if virus scanner is customized)
3	Copy file to conversion server	• Synchronous RFC connection • Configured path to data storage before and after conversion For more information, see the *Data Storage Security* subsection.
4	Create thumbnail and preview	Standard Web service for the SAP NetWeaver Portal You can restrict the access rights for this service through a a standard SAP NetWeaver Portal mechanism.
5	Store data on content server (file, thumbnail, preview)	• Synchronous RFC connection • Logical path and file names For more information, see the *Using Logical Path and Filenames to Protect Access to the File System* subsection.

If you use the Internet Graphics Service with DAM, refer to the corresponding security information in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide* > *Special Topics* > *Internet Graphics Service Security*.

A conversion Web service from a third party can affect the security of your solution. Refer to the security guidelines of the vendor and ensure that the Web service interface as well as the conversion file storage is protected from unauthorized access.

User Administration and Authentication

User Management

DAM requires user management settings in the SAP NetWeaver Portal and in the CRM backend system. Note that the authorization Customizing in the backend system affects the user role for the SAP NetWeaver Portal. Ensure that the authorizations granted in the backend system enable the user to carry out the processes that are part of the user's SAP NetWeaver Portal role.

You must define the user roles according to your business requirements. For example, some administrative functions should only be accessible to administrators because they provide access to data without further security checks.

User Types

The following user types are required for using DAM:

- Individual users

  For DAM processes, such as upload, download, and administration, dialog users are used. The standard system does not contain users or user roles for DAM. The users in SAP NetWeaver Portal have to be mapped to the corresponding backend users in SAP CRM.
- Technical users

  Service users are used for indexing the sources through TREX.

  You must map the `INDEX_SERVICE` standard service user that is used in Knowledge Management in SAP NetWeaver Portal to the DAM index service users in the SAP CRM backend system:

  1. Create a DAM index service user
  2. Create a user assignment for the Knowledge Management service user in the SAP NetWeaver Portal.
  3. Assign the DAM index service user.

  For more information, see Customizing for *Customer Relationship Management* under *Transaction CRMC_MKT_DAM* › *Maintain General Settings in DAM* › *Documentation for user parameter CRM_DAM_SERVICE_USER* .

Authorizations

To use DAM, you must configure at least one authorization role in the SAP CRM backend system. The authorization role must include the authorizations for the underlying components. To use DAM, users must be granted authorizations for the underlying components of the following authorization objects:

- `B_USERST_T`
- `B_USERSTAT`
- `C_CABN`
- `C_TCLA_BKA`
- `C_KLAH_BKP`
- `S_DATASET`
- `B_BUPA_RLT`
- `CRM_ORD_LP`
- `CRM_ORD_OE`

- CRM_ORD_PR
- CRM_SAO

  This authorization object is relevant only if you use the shipped BAdI implementation examples.

To check for additional authorization checks that the underlying components may have introduced in the meantime, check the list using an authorization trace. For example, you can use the authorization trace in the *System Trace* (ST01) transaction.

> **Note**
>
> Without creating the necessary authorizations, you cannot use DAM.
>
> For more information, see Customizing for *Customer Relationship Management* under ▶ *Transaction CRMC_MKT_DAM* › *Security and Authorization Concept* › *Security and Authorizations* ◀.

The DAM repository is integrated in the Knowledge Management (KM) framework of the SAP NetWeaver Portal. You can use standard KM iViews, such as the iViews for navigation and search to find digital asset versions that are provided as documents. To control the access to digital asset versions, you can use the content filter for DAM in SAP CRM. For more information, see the installation guide for SAP CRM on SAP Service Marketplace at service.sap.com/instguides.

The authorization concept of DAM is based on the attributes of digital asset versions, for example the attributes for displaying and editing digital assets. Authorization checks that are based on the attributes of digital asset versions use the authorization object DAM_ASSET.

Standard Authorization Objects

The following table shows the authorization objects that are relevant for security settings in DAM:

Table 128

Authorization Object	Field	Description
DAM_ASSET	ACTVT	Activity, for example read or change
	DAMDOCTYPE	Asset type, for example picture, video, manual
	PHIOSTATE	Asset status, for example new, in process, released
	PHIOSECSTATE	Asset security level, for example public or confidential
	PROPERTY_1 to PROPERTY_5	Attributes of digital assets and digital asset versions that can be used as further aspects for authorization checks
DAM_ASSACC	DAM_ACCWAY	Allowed asset access types: • Download • Streaming • File transfer protocol (FTP) • Mass update
DAM_RELASS	DAM_RELLOC	Unlocking of locked assets

Authorization Object	Field	Description
		If you choose the field value X, the user is allowed to unlock locked assets. If you leave the field empty, the user is not allowed to unlock locked assets.

Network and Communication Security

Communication Channel Security

The following figure shows the communication paths and communication protocols that are used in the DAM scenario. The graphic is followed by a table stating the communication paths and communication protocols that are used:

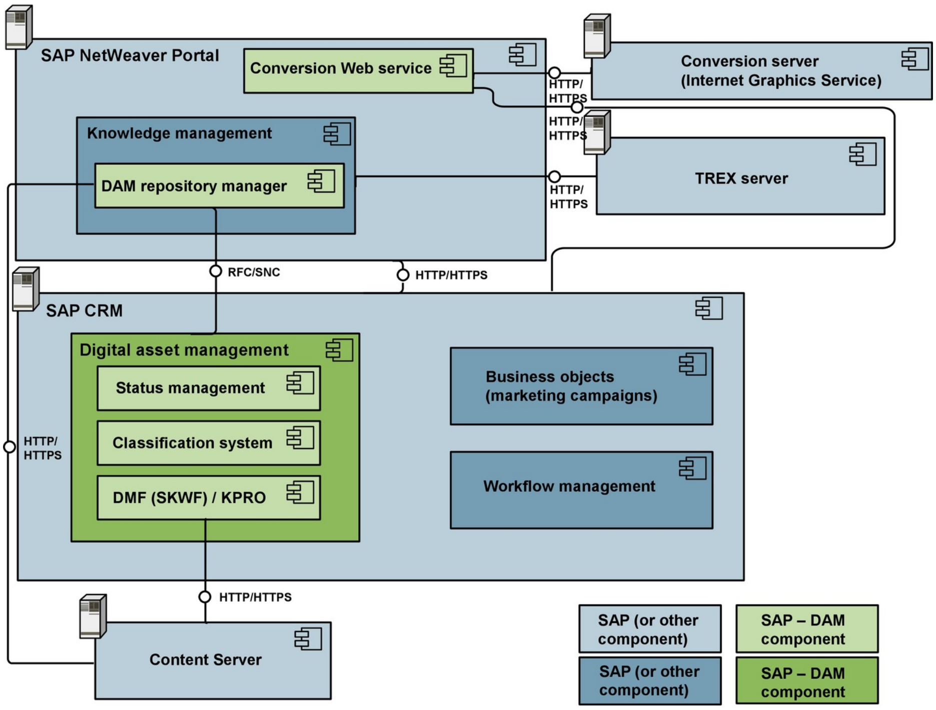


Figure 11: Communication Paths and Communication Protocols for Digital Asset Management

Table 129

Component A of DAM Scenario	Component B of DAM Scenario	Channel	Protocol Used
SAP NetWeaver Portal (DAM conversion Web service)	Conversion server (optional, for example Internet Graphics Service)	Server to server	HTTP or HTTPS
SAP NetWeaver Portal (DAM conversion Web service)	SAP CRM	Server to server	HTTP or HTTPS
SAP NetWeaver Portal – Knowledge Management (DAM repository manager)	Content server	Server to server	HTTP or HTTPS

Component A of DAM Scenario	Component B of DAM Scenario	Channel	Protocol Used
SAP NetWeaver Portal – Knowledge Management (DAM repository manager)	SAP CRM (DAM)	Server to server	RFC/SNC
SAP NetWeaver Portal – Knowledge Management	TREX	Server to server	HTTP or HTTPS
SAP NetWeaver Portal	SAP CRM	Server to server	HTTP or HTTPS

Communication Destinations

An iView property of DAM iViews contains information about the backend systems that the iView communicates with, such as the SAP CRM backend system or the TREX server. The iView property usually contains the system landscape alias shipped with SAP CRM.

DAM uses two RFC Destinations for the conversion service. These RFC destinations have to be configured in the *Configuration of RFC Connections* transaction (SM59) and named in the general settings of DAM.

For more information, see the installation guide for SAP CRM on SAP Service Marketplace at service.sap.com/instguides.

Internet Communication Framework Security

Activate only services that are required by the applications that are part of your system. For DAM, the service CRMDAM is required. To activate this service, use transaction SICF. For more information, see the following references:

- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Activating and Deactivating ICF Services*.
- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for Connectivity and Interoperability Technologies* › *RFC/ICF Security Guide*

Data Storage Security

DAM stores information in several places. For the security aspects regarding the data storage refer to the following security guides:

- *SAP Content Server Security Guide*

  SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *SAP Content Server Security Guide*.
- *Search and Classification (TREX) Security Guide*

  SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Search and Classification (TREX) Security Guide*.
- *Knowledge Management Security Guide*

  SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Knowledge Management Security Guide*.

Server directories temporarily contain the converted files. For the directory name, see the following entries in the general settings for DAM:

- `CONV_INCOMING_DIR`
- `CONV_OUTGOING_DIR`

To protect these directories from unauthorized access, we recommend that you use the available access restrictions by the operating system, network, firewalls, and so on.

Using Logical Path and Filenames to Protect Access to the File System

DAM saves data in files in the file system. Therefore, you must explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs. The following lists show the logical file names and paths used by Digital Asset Management and for which programs these file names and paths apply:

Logical File Names Used in Digital Asset Management for Upload of Files

The following logical file names have been created to enable the validation of physical file names during the upload of files:

- `CRM_DAM_TMP_UPLOAD_FILE`
  - Programs using this logical file name:
    - Class `CL_CRM_DAM_ASSET` and method `CREATE_FROM_FRONTEND`
    - Class `CL_CRM_DAM_ASSET_GENERAL` and method `CREATE_FILE_ON_SERVER`
    - Class `CL_CRM_DAM_BSP_MUPL_CONTRL` and method `CREATE_PACKAGE_WISE`
  - Parameters used in this context:

    <temporary physical file name>: This is a GUID created by the application individually for each file.
- `CRM_DAM_TMP_UPLOAD_FILE2`
  - Programs using this logical file name:
    - Class `CL_CRM_DAM_ASSET_GENERAL` and method `CREATE_FILE_ON_SERVER`
    - Class `CL_CRM_DAM_ASSET_GENERAL` and method `CONVERT_ASSET`
    - Class `CL_CRM_DAM_ASSET_VERSION` and method `STORE_WITH_FILE`
    - Function module `CRM_DAM_COPY_FILE_TO_DEST`
  - Parameters used in this context:

    <temporary physical file name>: This is a GUID created by the application individually for each file.

Logical Path Names Used in Digital Asset Management for Upload of Files

The logical file names listed above all use the logical file path `CRM_DAM_TMP_UPLOAD_PATH`.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log. For more information, see the following references:

- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *Function-Oriented View*: Search for *Logical File Names*.
- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* >

Security Guides for the Application Server › *Security Guides for the AS ABAP* › *SAP NetWeaver Application Server ABAP Security Guide* › *Special Topics* › *Protecting Access to the File System Using Logical Path and File Names* ›

- SAP Library for SAP NetWeaver on SAP Help Portal at › help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ›: Search for *Security Audit Log*.

Trace and Log Files

If a file upload is stopped because of a virus, CRM application log entries are written. For more information, see the following entries in the application log:

- Object assignment `CRM_DAM`
- Subobject assignment `CRM_DAM_MASS_UPL`

The log entries for DAM for Java iViews are written to the standard log files of the Java application server (AS Java). The following trace locations are contained in the standard system:

- `com.sap.portal.crmdamjca_logger`
- `com.sap.portal.crmdamnavigation_logger`
- `com.sap.portal.crmdamrm_logger`
- `com.sap.portal.dam_AssetIdentification_logger`
- `com.sap.portal.dam_add2basket_logger`
- `com.sap.portal.dam_authorization_logger`
- `com.sap.portal.dam_basket_logger`
- `com.sap.portal.dam_conversion_iview_logger`
- `com.sap.portal.dam_conversion_service_logger`
- `com.sap.portal.dam_lidetail_logger`
- `com.sap.portal.dam_logger`
- `com.sap.portal.dam_singledownload_logger`

For more information about configuring log and trace levels, see SAP Library for SAP NetWeaver on SAP Help Portal at › help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ›: Search for *Logging and Tracing*.

Checklist

The following table contains security aspects for DAM and provides information on how to ensure that the corresponding security settings are in place:

Table 130

Security Aspect	What to Check	How to Check
Authorization Customizing of backend roles	Is the access to the digital assets restricted as required?	Perform searches and qualifications to test whether the desired restrictions apply.
Portal role Customizing	Is the access to Portal iViews restricted as required?	Some iViews in SAP NetWeaver Portal in the areas Knowledge Management and DAM administration do not filter the requested information using the DAM authorization objects. Check if these

Security Aspect	What to Check	How to Check
		iViews are accessible for administrators only.
Virus checker installation	Does the system check files to be uploaded for viruses?	Try to upload the `EICAR` test virus.

3.1.17 Creation of a Campaign and Target Group from an External System

SAP CRM 7.0 EHP3 supports the creation of a campaign in SAP CRM from an external system by implementing the new RFC service *Creation of a Campaign and Target Group from an External System*. The service consumer can provide a list of external users, such as social media users from the service interface. The RFC service uses external list management (ELM) to create a target group. This target group contains a list of marketing prospects that corresponds to the list of external users that was transferred. The target group is assigned to the campaign. The service consumer can request the creation of an SAP Jam group that contains links to the target group and campaign in SAP CRM.

Why Is Security Necessary?

The RFC service uses several applications from SAP CRM and allows the usage of SAP Jam. This raises some application-specific security aspects and aspects of the SAP Jam integration with SAP CRM that may be relevant to the security of your SAP CRM system.

Before You Start

Fundamental Security Guides

In addition refer to the following section of the SAP CRM security guide:

- External List Management [page 72]
- Marketing Prospects [page 74]
- Segmentation [page 74]
- Campaign Management [page 80]
- Further Topics [page 196] (*Integration of Social Collaboration with SAP CRM*

User Administration and Authentication

This RFC service uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, specifically the SAP NetWeaver 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 this RFC service.

For more information, see the *SAP NetWeaver Application Server ABAP Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP*.

If you are using SAP Jam with this RFC service, you also require an SAP Jam user.

The service is called using an RFC interface. The user that is logged on when performing the remote function call is referred to as the *RFC logon user* in the following text. The service starts certain background processing units and uses SAP business workflows that also include some background processing. The background processes are executed with the *WF-Batch user*.

As a result of the background processing, you have two different users, the *RFC logon user* and the WF-Batch user who both access SAP Jam via the ABAP API if you are using SAP Jam with this RFC service.

If you are using SAP Jam with this RFC service, check that you have created a user in SAP Jam that is based on the e-mail address for the WF-Batch user. The same e-mail address has to be assigned to the RFC logon user. You actually have two different SAP CRM users who are both authenticated as the same SAP Jam user. The reason for this is described in chapter *Authorizations*.

User Management

User management for this RFC service uses the mechanisms provided with the SAP NetWeaver Application Server ABAP, for example, tools, user types, and password policies.

If you are using SAP Jam with this RFC service, check that you have created a user in SAP Jam that is based on the e-mail address for the WF-Batch user. The same e-mail address has to be assigned to the *RFC logon user*.

We provide a list of the standard users required to operate this RFC service.

Standard Users

Table 131

System	User ID	Type	Password	Description
SAP CRM	WF-Batch	System user	-	WF-Batch is used in local background RFCs and SAP Business Workflow

Authorizations

This RFC service uses the authorization concept provided by the SAP NetWeaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to this RFC service.

When calling the service function modules from a remote system, an implicit authorization check is performed by SAP NetWeaver AS ABAP. For more information, see RFC Scenarios.

For more information, see SAP Library on SAP Help Portal at help.sap.com/netweaver under *SAP NetWeaver Platform* > *<Choose relevant release>* > *Security Information* > *Security Guide* > *SAP NetWeaver Security Guide* > *Security Guides for Connectivity and Interoperability Technologies* > *RFC/ICF Security Guide* > *RFC Scenarios*.

For setting up the required authorizations, see the following RFC modules used for the service interface and the corresponding function group:

Function group: CRM_SME_MC_RFC

Function Modules:

- CRM_SME_MC_START_CREATE_GROUP (if you are using SAP Jam)
- CRM_SME_MC_START_REUSING_GROUP (if you are using SAP Jam)
- CRM_SME_MC_START_WITHOUT_GROUP
- CRM_SME_MC_ADD_CONTACTS
- CRM_SME_MC_PROCESS_LIST
- CRM_SME_MC_GET_INFO

The access to information stored in SAP Jam groups is restricted by the SAP Jam authorization concept. Security information about SAP Jam is available on request.

SAP Jam provides multiple privacy levels for groups that define the following:

- Invite policy: who is allowed to invite additional participants to the group and in doing so extend the list of users with access to the information in the group
- Upload policy: who is allowed to upload content to the group
- Participation: who can view, create, edit, download, or upload group content

Observe the following when setting up your business processes:

The SAP Jam user with the e-mail address for the SAP CRM user WF-Batch creates the SAP Jam groups for the RFC service. If you want to allow invitations of new participants to the SAP Jam group from other SAP Jam users, specifically the user of the application consuming the RFC service, you cannot use the highest possible privacy level for the SAP Jam group. The highest possible privacy level allows only invitations by group administrators.

If you want to use the highest possible privacy level for the SAP Jam groups you should consider implementing the method *ADJUST_GROUP* for the *BAdI: Change Campaign and Further Processing* in Customizing for *Customer Relationship Management* under ▶ *Marketing* › *Creation of a Campaign and Target Group from an External System* › *Business Add-Ins (BAdIs)* ◀. This gives you the option of implementing the invitation of additional participants, such as business partners for the campaign. The method is executed by SAP CRM user WF-Batch at runtime.

Define the privacy level of the SAP Jam groups created by the RFC service in Customizing for *Customer Relationship Management* under ▶ *Marketing* › *Creation of a Campaign and Target Group from an External System* › *Define Scenario for Creating a Campaign from an External System* ◀.

In this Customizing activity, you can set the attribute *Sharing State* to define whether any group participant is allowed to invite others or whether additional participants can only be invited by the group owner.

Role and Authorization Concept for This RFC Service

The RFC service performs the following actions implicating the need for specific user authorizations:

- Access SAP Jam (If you are using the service with SAP Jam)
- Create text files in the file system of the application server
- Use External List Management
- Create and change SAP CRM campaign

SAP Jam is accessed by the *RFC logon user* and the background user WF-Batch but there is not a requirement for specific authorizations.

The other actions listed above are performed by the background user WF-Batch.The authorizations required by the user WF-Batch to use External List Management are described in the section *External List Management* of this Guide.The authorizations needed by the user WF-Batch to create or change a campaign are described in the section *Campaign Management* of this Guide.

The authorization required by the user WF-Batch to create text files is described in the following table:

Standard Authorization Objects

Table 132

Authorization Object	Field	Value	Description
S_DATASET	ACTVT	34	Write authorization for file access

You can check the authorizations required for the RFC service modules in transaction SU22 by filtering for function modules with names starting with *CRM_SME_MC_*.

Communication Destinations

For this RFC service you need a local background RFC inbound destination that supports queue names with the prefix “SOC_”. Enter this local background RFC inbound destination in Customizing for *Customer Relationship*

Management under ▶ *Marketing* › *Creation of a Campaign from an External System* › *Define Scenario for Creating a Campaign from an External System* ◀.

Data Storage Security

Data Storage

The RFC service temporarily stores a text file in the file system of the application server. This text file is the data source for ELM, which is used during RFC service processing. If the RFC service call was completed successfully, the file is deleted at the end of RFC service processing.

Using Logical Path and Filenames to Protect Access to the File System

Specify the logical file path for the storage of the temporary ELM file in Customizing for *Customer Relationship Management* under ▶ *Marketing* › *Creation of a Campaign from an External System* › *Define Scenario for Creating a Campaign from an External System* ◀.

3.2 Sales

This area in SAP Customer Relationship Management (SAP CRM) enables you to manage your sales cycle, from creating appointments and business opportunities to managing sales orders, contracts, and invoicing. It also allows you to organize and structure your sales territories according to your business requirements.

ABAP Stack Standard Roles Used by SAP CRM Sales

Table 133

Role	Description
`SAP_CRM_UIU_SLS_PROFESSIONAL`	PFCG Role for Sales Professional
`SAP_CRM_UIU_SPL_PROFESSIONAL`	PFCG Role for Service Parts Logistics Management Professional

3.2.1 Account Planning

The account planning application allows you to maintain account plans. An account plan can be created and maintained both online and offline and is used to plan long term, nonpromoted sales for a planning account. It integrates key figure planning and allows you to view related trade promotions.

Account planning uses SAP NetWeaver Application Server (SAP NetWeaver AS) and SAP NetWeaver Business Warehouse (SAP NetWeaver BW).

Security Aspects of Data, Data Flow and Processes

For dialog users, the communication between the WebClient UI and the SAP CRM back end is established with the assignment to a business role and the corresponding PFCG role, communication protocol HTTP/HTTPS.

Account planning use the SAP BW planning services and uses synchronous RFC to retrieve and save planning data.

Business Roles

Table 134

Business Role	PFCG Role	Description
SPL	SAP_CRM_UIU_SPL_PROFESSIONAL	PFCG Role for Service Parts Logistics Management Professional
SALESPRO	SAP_CRM_UIU_SLS_PROFESSIONAL	PFCG Role for Sales Professional

User Management and Authentication

Account planning uses the normal user management of SAP NetWeaver AS and requires dialog users.

Key figure planning involves online updates of data in SAP NetWeaver BW. This requires a remote function call (RFC) connection with a user and password. In Customizing, the RFC user can be set to the current dialog user instead of a default RFC user, allowing for individual authorizations.

Users

Table 135

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary
SAP NetWeaver BW	Normal user	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations depending on the type of the marketing project (account plan or trade promotion) involving the employee responsible as a central entity. These authorization objects include the following:

Table 136

Authorization Object	Description
CRM_APL	SAP CRM Account Planning Authorization Object
CRM_APLAUG	Account Planning Authorization Group
CRM_APLRES	Account Planning Responsible Person
CRM_TPM	SAP CRM Marketing: Business Object Trade
CRM_TPMAGR	SAP CRM Marketing: Campaign Authorization Group
CRM_TPMCTP	SAP CRM Marketing: Campaign Type
CRM_TPMRES	SAP CRM Marketing: Person Responsible for Trade
CRM_TPMVER	SAP CRM Marketing: Authorization Object for Viewing the Version Data

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for account plans in ACE Customizing, because the rules that are delivered are dummy rules. For more information, see the Access Control Engine [page 324] section.

Network and Communication Security

Communication Channel Security

For information about communication channel security, see ▶ *Sales* ▶ *Communication Channel Security* ◀. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 137

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP (Secure sockets layer (SSL))	General data

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 138

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver BW	No	RFC	User, password	Additional SAP system for data evaluation
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, the appropriate rights – read, write, change, and delete – are required. There is no need for special data storage security.

Checklist

Table 139

Feature	Check	How to Check
Change an account plan or some of its properties	User settings for the account plan authorization objects	You can only make changes if you have the proper authorization.
View trade promotions related to an account plan	User settings for the account plan and trade promotion authorization objects	The trade promotions are only visible if you have the proper authorization.
Enter and save key figures for planning	Customizing for RFC destinations	If a dialog user has been maintained, you can only make changes if you have the proper authorization.

3.2.2 Activity Management

Activity management is an integral part of SAP Customer Relationship Management (SAP CRM) because it manages all activities undertaken by the employees of your company. Any data saved in an activity is an important source of information that needs to be accessed by all relevant employees.

You can use activity management at any time during the SAP CRM lifecycle. Activities such as interaction logs and appointments keep a record of any interaction that has taken place between your company and its customers.

Tasks provide a way for your employees to manage their own workload and to record reminders. You can mark appointments, interaction logs, and tasks as private. So, everything undertaken by employees within a department or company can be managed quickly and easily in one transaction.

User Management and Authentication

This application uses the user management and authentication mechanisms of SAP NetWeaver, in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP). For information about the applicable security recommendations and guidelines for user administration and authentication, see the *SAP NetWeaver Application Server ABAP Security Guide*.

User Management

Table 140

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (SU01) transaction and the profile generator (PFCG) transaction	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for activity management:

Table 141

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access activity management applications and Customizing for activity management. Created by an SAP CRM system administrator.

Authorizations

This application uses SAP NetWeaver Application Server (SAP NetWeaver AS) authorization. For information about applicable authorization recommendations and guidelines for this application, see the *SAP NetWeaver Application Server ABAP Security Guide.*

The SAP NetWeaver AS authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (PFCG) transaction on SAP NetWeaver AS ABAP.

For information about the authorization procedure used in this application, see Component-Specific Guidelines: SAP CRM [page 68].

The following table details the authorization objects for activity management:

Table 142

Authorization Object	Field	Description
CRM_ORD_OP	PARTN_FCT (partner function) PARTN_FCTT (partner function category) ACTVT (Activity)	Own documents
CRM_ORD_LP	CHECK_LEV PR_TYPE ACTVT (Activity)	Visibility in the organizational model
CRM_ORD_TE	PR_TYPE (Process Type) TERR_ASSGN (Territory Assignment, Direct/Higher Level) ACTVT (Activity)	Authorization Object CRM Order-Visibility in Territory
CRM_ACT	ACTVT (Activity)	Authorization Object CRM Order-Business Object Activity
CRM_ORD_PR	PR_Type (transaction type) ACTVT (Activity)	Business Transaction Type
CRM_ORD_OE	SALES_ORG (sales organization) SERVICE_OR (service organization) DIS_CHANNE (distribution channel) SALES_OFFI (sales office) SALES_GROU (sales group) ACTVT (activity)	Allowed organizational units
CRM_TERRMA	PATH_ID (territory hierarchy ID) ACTVT (Activity)	Territory processing
CRM_TXT_ID	TEXTOBJECT (texts: application object) TEXTID (text ID) ACTVT (Activity)	Display and edit texts
CRM_FLDCHK	ACTVT AUGRP (Authorization Group) LEVEL1 (Authorization Level)	CRM Order Authorization Object-Field Check

Network and Communication Security

The network topology for this application is based on the SAP NetWeaver platform and SAP CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 143

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to SAP CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as customer data
Front-end client using a Web browser to SAP CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as customer data

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the above section *Communication Channel Security*:

Table 144

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

3.2.3 Activity Journals

Activity journals are used in activities to record and update information gathered from customer visits or telephone calls. The information in the activity journal can be product-related.

User Management and Authentication

This application uses the user management and authentication mechanisms of SAP NetWeaver, in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP). For information about the applicable security recommendations and guidelines for user administration and authentication, see the *SAP NetWeaver Application Server ABAP Security Guide*.

User Management

Table 145

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (SU01) transaction and the profile generator (PFCG) transaction	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for activity journals:

Table 146

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	End user	No	Dialog user	No	Mandatory user who can access activity journals applications and Customizing for activity journals. Created by an SAP CRM system administrator.

Authorizations

This application uses SAP NetWeaver Application Server (SAP NetWeaver AS) authorization. For information about applicable authorization recommendations and guidelines for this application, see the *SAP NetWeaver Application Server ABAP Security Guide*.

The SAP NetWeaver AS authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (PFCG) transaction on SAP NetWeaver AS ABAP.

For information about the authorization procedure used in this application, see Component-Specific Guidelines: SAP CRM [page 68].

The following table details the authorization objects for activity journals:

Table 147

Authorization Object	Field	Description
CRM_ACTJNL	ACTVT (Activity) JNLTYPE (Type/Template)	Authorization Object CRM: Activity Journals

Network and Communication Security

Network Security

The network topology for this application is based on the SAP NetWeaver platform and SAP CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about Communication Channel Security, see the section *Communication Channel Security* in the section Network and Communication Security [page 29].

The following table lists the general communication paths used by SAP CRM, the protocol used for the connection, and the type of data transferred:

Table 148

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as credit card information, customer data, conditions, and so on
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as credit card information, customer data, conditions, and so on

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the section above *Communication Channel Security*:

Table 149

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

3.2.4 Activity Scheduling

Activity scheduling is used to generate activities with business partners and contacts. Activity proposals are based on the employee’s working hours, visiting hours defined for the business partners and contacts, and existing activities. The activity proposals appear in the calendar, and you can accept, reject, or reschedule them.

User Management and Authentication

This application uses the user management and authentication mechanisms of SAP NetWeaver, in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP). For information about the applicable security recommendations and guidelines for user administration and authentication, see the *SAP NetWeaver Application Server ABAP Security Guide*.

User Management

Table 150

Tool	Description
User and role administration with *SAP NetWeaver AS ABAP*: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for activity scheduling:

Table 151

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	End user	No	Dialog	No	Mandatory user who can access the activity scheduling application and Customizing for activity scheduling. Created by an SAP CRM system administrator.

Authorizations

This application uses SAP NetWeaver Application Server (SAP NetWeaver AS) authorization. For information about applicable authorization recommendations and guidelines for this application, see the *SAP NetWeaver Application Server ABAP Security Guide.*

The SAP NetWeaver AS authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (`PFCG`) transaction on SAP NetWeaver AS ABAP.

Activity scheduling does not have its own authorization object. Since activity scheduling is a preparatory step for the activities Activity Journals and Visit Planning, you must take into account the related authorization objects.

Network and Communication Security

The network topology for this application is based on the SAP NetWeaver platform and SAP CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 152

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as customer data
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as customer data

Network Security

For more information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the section above *Communication Channel Security*:

Table 153

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

3.2.5 Visit Planning

Visit planning supports sales representatives, account managers, and back-office employees in scheduling and carrying out interactions with accounts. Accounts can be grouped into visit plans according to certain criteria, such as location.

User Management and Authentication

Visit planning uses the user management and authentication mechanisms of SAP NetWeaver, in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 visit planning.

User Management

Table 154

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (SU01) transaction and the profile generator (PFCG) transaction.	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for visit planning:

Table 155

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	End user	No	Dialog user	No	Mandatory user who can access the visit planning application and Customizing for visit planning. Created by an SAP CRM system administrator.

Authorizations

This application uses SAP NetWeaver Application Server (SAP NetWeaver AS) authorization. For information about applicable authorization recommendations and guidelines for this application, see the *SAP NetWeaver Application Server ABAP Security Guide.*

The SAP NetWeaver AS authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (PFCG) transaction on SAP NetWeaver AS ABAP.

The following table details the authorization objects for visit planning:

Table 156

Authorization Object	Field	Description
CRM_TOUR	Path_ID (Territory Hierarchy ID) ACTVT (Activity)	Tour Maintenance

Network and Communication Security

The network topology for this application is based on the SAP NetWeaver platform and CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 157

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as customer data
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as customer data

Network Security

For more information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the section above *Communication Channel Security*:

Table 158

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

3.2.6 Opportunity Management

Opportunity management is a part of SAP Customer Relationship Management (SAP CRM) that enables you to control your sales process. You can also do this in the CRM Mobile Application (CRM Mobile), partner channel management, and the interaction center.

Opportunity management provides the framework for presenting sales projects from the very start and tracking their progress. In this way, it provides the basis for an analysis and optimization of your enterprise. Opportunity management is particularly useful in the following scenarios:

- Many sales representatives work for you
- Distribution of large sales order values
- The sales cycle spans a long time period of time

Opportunity management allows you to construct a sales methodology to suit your sales processes. Your sales employees are coached through the steps of an ideal sales process, from identifying the lead to closing the sale.

User Management and Authentication

Opportunity management uses the user management and authentication mechanisms of SAP NetWeaver; in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 opportunity management.

User Management

Table 159

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for opportunity management:

Table 160

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access the opportunity management application and Customizing for opportunity management. Created by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user for communication with the ERP server for response messages from SAP ERP. Created by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	The same remote function call (RFC) destination is used to communicate from SAP NetWeaver Business Warehouse (SAP NetWeaver BW) as for the other SAP CRM business objects. The user in the SAP CRM system who handles the requests from SAP NetWeaver BW to transfer data (user ALEREMOTE) needs to have two specific authorization objects: `CRM_ORD_LP` and `S_USER_GRP`. It is part of SAP NetWeaver BW authorization management to enforce proper authorization for SAP NetWeaver BW data so that users only see data for which they are authorized. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *SAP NetWeaver Business Warehouse*.
SAP ERP	Technical user	No	System user	No	Mandatory user for credit check. This user is only used with an RFC destination user. Created by an SAP ERP system administrator.

System	User	Delivered?	Type	Default Password	Description
SAP NetWeaver Business Warehouse (SAP NetWeaver BW)	Technical user	No	System user	No	Optional user for credit check with SAP Credit Management. This user is only used with an RFC destination user. Created by a system administrator in SAP NetWeaver BW.
SAP NetWeaver BW	Technical user	No	System user	No	Optional user for planning. This user is only used with an RFC destination user. Created by a system administrator in SAP NetWeaver BW.
SAP Strategic Enterprise Management (SAP SEM)	Technical user	No	System user	No	Optional user for planning. This user is only used with an RFC destination user. Created by an SAP SEM system administrator.

Authorizations

This application uses SAP NetWeaver Application Server (SAP NetWeaver AS) authorization. For information about applicable authorization recommendations and guidelines for this application, see the *SAP NetWeaver Application Server ABAP Security Guide.*

The SAP NetWeaver AS authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (`PFCG`) transaction on SAP NetWeaver AS ABAP.

For information about the authorization procedure used in this application, see Component-Specific Guidelines: SAP CRM [page 68].

The following table details the authorization objects for opportunity management:

Table 161

Authorization Object	Field	Description

`CRM_ORD_OP`	`PARTN_FCT (partner function)`
	`PARTN_FCTT (partner function category)`
	`ACTVT(Activity)`
		Own documents

`CRM_ORD_LP`	`CHECK_LEV`
	`PR_TYPE`
	`ACTVT` (Activity)
		Visibility in the organizational model

`CRM_ORD_TE`	`PR_TYPE` (Process Type) `TERR_ASSGN` (Territory Assignment, Direct/Higher Level) `ACTVT` (Activity)	Authorization Object CRM Order-Visibility in Territory

Authorization Object	Field	Description
CRM_OPP	ACTVT (Activity)	Authorization Object CRM Order-Business Object Opportunity
CRM_ORD_PR	PR_Type (Transaction type) ACTVT (Activity)	Business Transaction Type
CRM_ORD_OE	SALES_ORG (Sales organization) SERVICE_OR (Service organization) DIS_CHANNE (Distribution channel) SALES_OFFI (Sales office) SALES_GROU (Sales group) ACTVT (Activity)	Allowed organizational units
CRM_TERRMA	PATH_ID (territory hierarchy ID) ACTVT (Activity)	Territory processing
CRM_TXT_ID	TEXTOBJECT (texts: application object) TEXTID (text ID) ACTVT (Activity)	Display and edit texts
CRM_FLDCHK	ACTVT AUGRP (Authorization Group) LEVEL1 (Authorization Level)	CRM Order Authorization Object-Field Check

Network and Communication Security

The network topology for this application is based on the SAP NetWeaver platform and CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 162

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as customer data
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as customer data

Network Security

For more information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the section above *Communication Channel Security*:

Table 163

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

3.2.7 Organizational Management

Organizational management in SAP Customer Relationship Management (SAP CRM) offers you a flexible tool for displaying your company's task-related, functional organizational structure as a current organizational model.

Displaying your service or sales and distribution structure is at the forefront of SAP CRM. To work with the SAP CRM system, you can simply display the organizational units that are relevant for your sales and service-related processes.

Organizational management use SAP NetWeaver Application Server (SAP NetWeaver AS).

User Management and Authentication

Users

Table 164

System	User	Delivered?	Type	Default Password
SAP CRM	Normal user	No	Dialog user	Arbitrary

Authorization Objects

There are several authorization objects, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 165

Authorization Object	Description
`PLOG`	Controls authorization check for personal development data

Network and Communication Security

The network topology for this application is based on the SAP NetWeaver platform and CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 166

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as customer data
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as customer data

Network Security

For more information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the above section *Communication Channel Security*:

Table 167

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

3.2.8 Surveys

A survey is a type of questionnaire for gathering information from specific users.

Surveys are specialized forms that can be integrated into Web sites or sent as attachments in personalized e-mails to customers. The submitted answers are collected on a server and, depending on the business scenario, the results are either stored in a database or condensed beforehand. Later, the results are evaluated and can be used for making strategic decisions.

Surveys are an important means of gaining specific information from known and unknown users. For example, as part of a marketing campaign, you could use a survey to test the market before launching a new product, or as part of a customer satisfaction survey to gather feedback on a product already purchased. The results collected from surveys play an important role in making strategic decisions, for example, when planning a new product launch or when making improvements for future products.

User Management and Authentication

Surveys use the normal user management of SAP NetWeaver AS and require dialog users.

Users

Table 168

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Authorization Objects

The following authorization object is used for survey processing:

Table 169

Authorization Object	Authorization Field
CRM_SVY	ACTVT

> **Note**
>
> A new authorization check using authorization object CRM_SVY is available with SAP Note 1480248. You must check and update the authorization profiles for users working with surveys, as required.

In addition, access checks are made based on PFCG roles. Currently, surveys are enabled in the interaction center user interface for the *Marketing Professional* and *Service Professional* roles.

Network and Communication Security

Communication Channel Security

Table 170

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP(SSL)	General data

For more information about communication channel security, see Network and Communication Security [page 29].

Network Security

For information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 171

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, no special data storage security measures are required. Surveys are a dependent application, so the leading application storage security applies to survey read or edit rights.

Checklist

Table 172

Feature	Check	How to Check
View or maintain surveys	Does the PFCG role allow access to the survey application?	Role assignment
View or maintain surveys	Leading object checks for read or edit rights for surveys	Leading object (for example, an opportunity or lead)

3.2.9 Survey Suite

You can use Survey Suite to create and edit surveys. In the survey designer, you can do the following:

- Assign style sheets
- Switch between HTML and XML views
- Display and edit survey structures with sections, questions, and answers
- Assign answer options
- Display rating values

In the survey designer, the survey hierarchy is on the left side of the screen, and editing options for layout and formatting appear on the right side.

The hierarchy node you select to edit determines the following:

- Features that you can add to your survey. These are displayed in the block immediately above the hierarchy node.
- Editing options available. These are displayed on the right side of the screen.

User Management and Authentication

Survey Suite uses the normal user management of SAP NetWeaver AS and requires dialog users.

Users

Table 173

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Authorization Objects

No authorization objects exist. Access checks are made from PFCG roles.

Currently, the survey suite is enabled in the interaction center user interface for the *Marketing Professional* and *Service Professional* roles.

Network and Communication Security

Communication Channel Security

Table 174

Communication Path	Protocol Used	Type of Data Transferred
Internet	TCP/IP(SSL)	General data

For more information about communication channel security, see Network and Communication Security [page 29].

Network Security

For information about network security, see Network and Communication Security [page 29].

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the *Communication Channel Security* section above:

Table 175

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user, no special data storage security measures are required. Survey Suite is a dependent application, so the leading application storage security is also used for survey read or edit rights.

Checklist

Table 176

Feature	Check	How to Check
View or maintain survey	Does the PFCG role allow access to the survey application?	Role assignment

Feature	Check	How to Check
XML import of survey	File upload tag of THTMLB is used, virus checks are done	N/A

3.2.10 Territory Management

Territory Management enables an organization to structure and organize sales markets by dividing them into territories. This allows you to set up an optimal coverage model of sales territories by sales professionals, providing invaluable opportunities for organizations to drive profitable growth.

Territory Management uses SAP NetWeaver Application Server (SAP NetWeaver AS).

User Management and Authentication

This application uses the user management and authentication mechanisms of SAP NetWeaver, in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP). For information about the applicable security recommendations and guidelines for user administration and authentication, see the *SAP NetWeaver Application Server ABAP Security Guide*.

User Management

Table 177

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for activity management:

Table 178

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access activity management applications and Customizing for activity management. Created by an SAP CRM system administrator.

Authorization Objects

There are several authorization objects, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include:

Table 179

Authorization Object	Field	Description
CRM_TERRMA	PATH_ID (Territory Hierarchy ID) ACTVT (Activity)	Controls which territories the user can process
CRM_TERRDY	ACTVT (Activity) TERR_LEVEL (Scope of Territory Dynamic Authority Check)	Territory Management dynamic authorization check that controls which territories the user can process according to the assignment of the user in the territory tree structure
CRM_FDT	ACTVT (Activity) BRFP_APPL (Rule Policy Type ID)	Controls whether the user can create, display, change, or delete the rules

Network and Communication Security

The network topology for this application is based on the SAP NetWeaver platform and CRM Middleware topology. For information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the section Network and Communication Security [page 29].

Communication Channel Security

For more information about communication channel security, see Network and Communication Security [page 29]. The available communication paths, protocols used, and type of data transferred are listed in the following table:

Table 180

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to SAP CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as customer data
Front-end client using a Web browser to SAP CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as customer data

Communication Destinations

The following communication destinations can be reached using the communication paths listed in the above section *Communication Channel Security*:

Table 181

Destination	Delivered?	Type	User, Authorizations	Description
SAP NetWeaver AS	Yes	Dynamic Information and Action Gateway (DIAG)	User, password	N/A

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

Checklist

Table 182

Feature	Check	How to Check
View or maintain a territory	User settings for the territory authorization objects	If a user is not authorized to perform changes, the system rejects the changes.

3.2.11 Quotation and Order Management

You can use the sales transactions in SAP Customer Relationship Management (SAP CRM) to represent the business transactions in the sales area of your company. You can create, process, and post-process quotations and sales orders.

This section describes security issues specific to Quotation and Order Management, including the integration with Quotations of the SAP Price and Margin Management application by Vendavo.

Important SAP Notes

The most important SAP Notes that apply to the security of the Quotation and Order Management are shown in the table below.

Table 183

Title	SAP Note	Comment
RFC authorizations for sales order management	1428603	RFC authorizations relevant for sales order management
Logging of changes for external references tables	1424192	Tables related to the external references are enabled to log changes
No authorization check performed for attachments	1416683	Introduced authority check for handling of attachments in sales documents

Why Is Security Necessary?

Security is necessary because quotation and order management performs the following actions:

- Accesses master data, such as business partner information. This contains critical business information, such as leads, opportunities, and sales orders.

- Integrates from a central point with different systems, such as SAP ERP and SAP Advanced Planning and Optimization (SAP APO)
- Processes sensitive customer data, such as credit card information

User Administration and Authentication

Quotation and order management uses the user management and authentication mechanisms of SAP NetWeaver, in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 quotation and order management.

This section lists the tools for user management, types of users required, and standard users that are delivered.

User Management

User management for the Quotation and Order Management uses the mechanisms such as tools, user types, and password policies provided with the SAP NetWeaver Application Server ABAP. For an overview on how these mechanisms apply to Quotation and Order Management, see the sections below. A list of the standard users required for operating Quotation and Order Management is also provided.

Table 184

Tool	Detailed Description	Prerequisites
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information, see User Administration and Authentication [page 18].	None

User Types

It is often necessary to specify different security policies for different user types. For example, your policy may specify that individual users performing tasks interactively have to change their passwords on a regular basis whereas users running background processing jobs do not.

The user types required for Quotation and Order Management include:

- Individual users:
  - Dialog users are used for the WebClient UI
- Technical users
  - Service users are used for processing background jobs
  - Service users are used for executing functions in a connected SCM APO system (availability check)
  - Service users are used for executing functions in a connected SAP ERP system (availability check)
- Communication users are used for data exchange of business transactions with the connected SAP ERP system.
- Background users are used for background jobs.

For more information about user types, see the SAP NetWeaver AS ABAP Security Guide.

Standard Users

The following users must be created for quotation and order management:

Table 185

System	User	Delivered?	Type	Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access sales, presales, and billing transactions. Created by an SAP CRM system administrator.
SAP CRM	End user	No	System user	No	Mandatory user who can process background jobs. Created by an SAP CRM system administrator.
SAP ERP	All users	No	System user	No	Mandatory user for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, the user can be a personal user or a system RFC user. Created by an SAP ERP system administrator. For more information, see SAP Note 338537 .
SAP CRM	SAP APO user	No	System user or dialog user	No	Optional user for communication with APO server for availability check. Created by an SAP CRM system administrator.
SAP CRM	SAP ERP user	No	System user	No	Optional user for communication with the ERP

System	User	Delivered?	Type	Password	Description
					server for availability check. Created by an SAP CRM system administrator.
SAP ERP	All users	No	Dialog User	No	Optional user for displaying SAP ERP sales documents such as deliveries or invoices in the WebClient UI, using the transaction history

Authorizations

This application uses SAP NetWeaver Application Server (SAP NetWeaver AS) authorization. For information about applicable authorization recommendations and guidelines for this application, see the *SAP NetWeaver Application Server ABAP Security Guide.*

The SAP NetWeaver AS authorization concept assigns authorizations to users, and these authorizations are dependent on the user role. For role administration, use the profile generator (`PFCG`) transaction on SAP NetWeaver AS ABAP and the User Management Engine's user administration console on the AS Java.

Standard Roles

The table below shows the standard roles used by the Quotation and Order Management:

Table 186

Role	Description
`SalesPro`	Sales Professional Role
`SPL`	Sales Order Management in Service Parts Management Scenario

Standard Authorization Objects

The following table lists the security-relevant authorization objects that are used in quotation and order management:

Table 187

Authorization Object	Field	Value	Description

`CRM_ORD_OE`	`SALES_ORG` (sales organization)
	`SERVICE_OR` (service organization)
	`DIS_CHANNE` (distribution channel)
		`ACTV:`
		`01 = Create`
		`02 = Change`
		`03 = Display`
		`06 = Delete`
			Allowed organizational units

Authorization Object	Field	Value	Description
	SALES_OFFI (sales office) SALES_GROU (sales group) ACTVT (activity)		
CRM_ORD_PC	ACTVT PR_TYPE	ACTV: 02 = Change 03 = Display	Credit card processing
CRM_ORD_OP	PARTN_FCT (partner function) PARTN_FCTT (partner function category) ACTVT	ACTV: 02 = Change 03 = Display 06 = Delete	Own documents
CRM_ORD_PR	PR_TYPE (transaction type) ACTVT	ACTV: 01 = Create 02 = Change 03 = Display 06 = Delete	Business transaction type
CRM_SAO	ACTVT	ACTV: 45 = Allow	Business object – sales order
CRM_TERRMA	PATH_ID (territory hierarchy ID) ACTVT	-	Territory processing
CRM_TXT_ID	TEXTOBJECT (texts: application object) TEXTID (text ID) ACTVT	-	Display and edit texts
CRM_ORD_LP	CHECK_LEV PR_TYPE ACTVT	ACTV: 01 = Create 02 = Change 03 = Display 06 = Delete	Visibility in the organizational model

Network and Communication Security

The network topology for quotation and order management is based on the topology used by the SAP NetWeaver platform and CRM Middleware. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and in Network and Communication Security [page 29] also apply to quotation and order management.

Communication Channel Security

The following table lists the various communication channels that are used between the components of quotation and order management and other applications:

Table 188

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive SAP CRM data such as credit card information, customer data, and conditions
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive SAP CRM data such as credit card information, customer data, and conditions
CRM server to ERP server	RFC	System ID, client and host name, and all application data	System information and SAP CRM data
ERP server to CRM server	RFC	System ID, client and host name, and all application data	System information and SAP ERP data
CRM server to APO server	RFC	System ID, client and host name, and all application data	System information and SAP CRM data
CRM server to Business Intelligence (BI) server	RFC	System ID, client and host name, and all application data	System information and SAP CRM data
CRM server to Internet Pricing and Configurator (IPC)	RFC	Pricing conditions	System information and SAP CRM data
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and SAP CRM data
SAP CRM	Web Service	All application data according to service definition	System information and SAP CRM data

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

The following figure illustrates the communication paths listed in the table above:

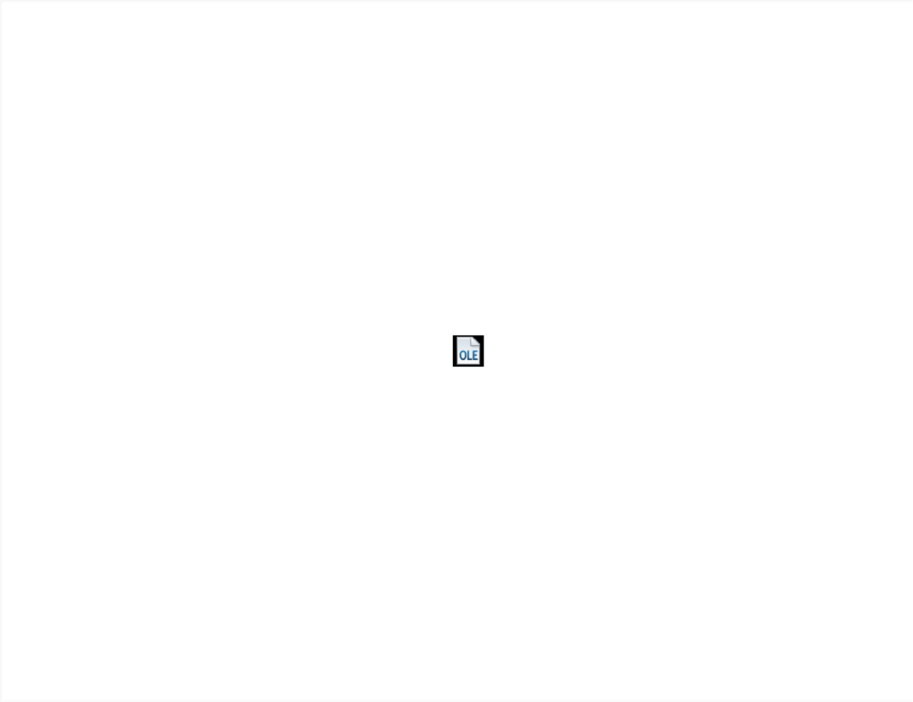


Figure 12: Communication Paths

Communication Destinations

The table below shows an overview of the communication destinations used by the quotation and order management:

Table 189

Destination	Delivered	Type	User Authorizations	Description
SAP ERP	No	RFC	Not Delivered	Connection for the middleware communication to SAP ERP, used for example, for sales order data exchange
SCM APO	No	RFC	Not delivered	Optional connection for availability check using SCM APO system
SAP ERP	No	RFC	Not delivered	Optional connection for SAP ERP based availability check
SAP ERP	No	RFC	Not delivered	Optional. In the case of SAP ERP sales documents such as invoices or deliveries that should be displayed on the

Destination	Delivered	Type	User Authorizations	Description
				WebClient UI (transaction history)

Data Storage Security

If credit card data is processed, credit card encryption is recommended. For more information, see section Payment Card Security According to PCI-DSS [page 42].

Checklist

Table 190

Feature	Check	How to Check
Availability check	What destination is used for the ATP check?	In Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Middleware Parameters* ◀.
Logon	What logon procedure is used for this destination?	Use *Configuration of RFC Connections* (transaction `SM59`)

3.2.12 Sales Contracts and Agreements

Sales contracts and agreements allow the customer to release products under specific, previously agreed-upon conditions.

For sales contracts and agreements the same guidelines apply as described in Quotation and Order Management [page 150]. There are exceptions in the following cases:

- Credit card processing is not used
- There is no integration with SAP Advanced Planning and Optimization (SAP APO)

Sales contracts and agreements use the following additional authorization objects:

Table 191

Authorization Object	Field	Description
`CRM_CO_SC`	`ACTVT`	Business Object Sales Contract
`CRM_OUTL`	`ACTVT`	Business Object Outline Agreement

3.2.13 Credit Analyst Workbench

The Credit Analyst Workbench processes the clearing of transactions that have the status *Credit not ok*. It is intended for users who are considered credit analysts from a business perspective.

The Credit Analyst Workbench is connected to an SAP ERP system, such as Financial Accounting, to obtain the necessary information (for example, the credit limit of a payer).

The Credit Analyst Workbench is a functional component used in the context of the SAP CRM sales cycle. This section describes security issues specific to the Credit Analyst Workbench only. For information about topics such as *User Management*, or *Network and Communication Security*, see the corresponding sections in the section *Introduction*.

Important SAP Notes

The most important SAP Notes that apply to the Credit Analyst Workbench security are shown in the table below:

Table 192

Title	SAP Note	Comment
Logging of changes for credit management tables	1428603	Enable logging of changes performed on tables pertaining to credit management

Authorizations

Authorization objects are required for preventing users without sufficient permissions from displaying or processing sales orders when they use the Credit Analyst Workbench. The table below shows the security-relevant authorization objects that are used in the Credit Analyst Workbench:

Table 193

Authorization Object	Field	Value	Description
CRM_CWB	CWB_CRG	Valid values are dependent on Customizing or application data	Credit Representative Group in Credit Management
CRM_CWB	CWB_RCL	Valid values are dependent on Customizing or application data	Risk Category

Communication Destinations

The RFC destination used in the Credit Analyst Workbench for connection to SAP ERP is maintained in the Customizing for the middleware settings. Use the transaction SM59 to maintain the logon procedures for the RFC destination.

3.2.14 ERP Sales Document Processing

SAP Customer Relationship Management (SAP CRM) offers a user interface to view and modify ERP sales documents (such as sales orders, customer quotations, and contracts) directly in a connected SAP ERP back-end system.

For this scenario, we recommend that you use a separate, trusted, remote function call (RFC) connection based on the current user. This allows you to set different authorization levels for each user. As a prerequisite, you must have counterpart users in SAP ERP with the same ID and the following PFCG role assigned:

Table 194

Role	Description
SAP_LO_SD_ORDER_MANAGEMENT	PFCG Role for Sales Professional on SAP ERP side

For information about credit card usage in ERP sales orders in SAP CRM, see Credit Card Usage Overview [page 43].

3.2.15 Billing in SAP CRM

Billing is an ABAP-based component that allows you to create customer invoices in SAP Customer Relationship Management (SAP CRM). Billing is integrated with SAP CRM scenarios.

The billing documents and the actual revenues can be posted in financial accounting and in controlling of SAP ERP Financials by using the standard integration between billing in SAP CRM and these components of SAP ERP Financials.

Why Is Security Necessary?

Security is necessary because billing in SAP CRM does the following:

- Accesses data in the CRM system, such as business partner information, and contains business information, such as invoices
- Has direct access to the tax engine and the pricing engine, where all products and prices are stored
- Is integrated with the financial accounting (FI) module of SAP ERP, which is important for financial service
- Processes sensitive customer data, such as credit card information

Security Aspect of Dataflow and Processes

The figure below shows an overview of the processes for the Billing in SAP CRM.

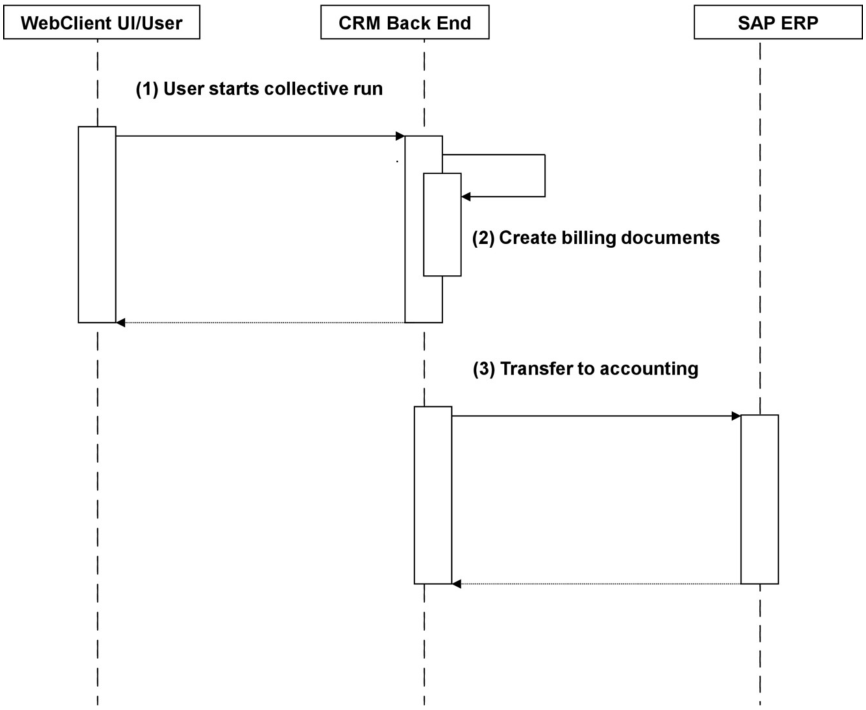

WebClient UI/User
CRM Back End
SAP ERP
(1) User starts collective run
(2) Create billing documents
(3) Transfer to accounting

Figure 13: Overview of Process Steps for Billing in SAP CRM

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

Table 195

Step	Description	Security Measure
1	User starts a collective run	User Type: Dialog user with assignment to business role and PFCG role, Communication Protocol, HTTP/HTTPS
2	System creates billing document	For more information, see the section *Authorizations*.
3	System transfers billing documents to Accounting	Asynchronous RFC based communication: Special security measures have been taken in case of credit card processing. For more information, see section Payment Card Security According to PCI-DSS [page 42].

User Administration and Authentication

Billing in SAP CRM uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP NetWeaver Application Server (SAP NetWeaver AS). 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 the billing component in SAP CRM.

User Management

User management for the billing component in SAP CRM uses the mechanisms provided by SAP NetWeaver AS ABAP, such as tools, user types, and password policies. For an overview of how these mechanisms apply to the application, see the following sections:

Table 196

Tool	Description
User and role administration with SAP NetWeaver AS: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction.	For more information, see User Administration and Authentication [page 18].

User Types

The following user types are required for billing in SAP CRM:

Table 197

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access billing transactions. Created by an SAP CRM system administrator.
SAP CRM	End user	No	System user	No	Mandatory user who can process background jobs.
SAP ERP	End user	No	System user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, user can be a personal user or a system RFC user. Created by an SAP ERP system administrator.

Authorizations

Billing in SAP CRM uses the authorization provided by SAP NetWeaver AS. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the billing component.

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

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for billing in ACE Customizing, because the rules in the SAP standard system are dummy rules. For more information, see the Access Control Engine [page 324] section.

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the billing component in SAP CRM:

Table 198

Authorization Object	Field	Description
BEA_DLI	ACTVT APPL BILL_ORG BILL_TYPE	Maintenance of the billing due list
BEA_BDH	ACTVT APPL BILL_ORG BILL_TYPE	Creation and maintenance of billing
BEA_SUBS	ACTVT APPL BILL_TYPE	Display of documents in SAP ERP

Network and Communication Security

The network topology for billing in SAP CRM is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM.

Communication Channel Security

The following table lists the various communication channels that are used between the billing component and other applications:

Table 199

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data, and credit card data.
ERP server to CRM server	RFC	System ID, client, and host name, and all application data	System information and ERP data
CRM server to business intelligence (BI) server	RFC	System ID, client, and host name, and all application data	System information and CRM data
CRM server to Internet Pricing and Configurator (IPC) (Necessary only if IPC runs on a separate installation; See SAP Note 855455.)	RFC	Pricing conditions	System information and CRM data

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data
CRM server to global trade services (GTS) server	RFC	System ID, client, and host name, and all application data	System information and CRM data

In most cases, only application data is sent across (billing due list DLI and billing document BDH/BDI).

- The following data is received from SAP ERP:
  - Delivery documents
  - Inspection documents
  - Status feedback, payout data, and payment data from FI
- The following data is received from SAP CRM:
  - Service orders
  - Service contracts
  - Sales orders
  - Sales contracts
  - Claims

Data Storage Security

If credit card data is processed, credit card encryption is recommended. For more information, see section Payment Card Security According to PCI-DSS [page 42].

Important SAP Notes

Table 200

SAP Note Number	Short Text
1246835	S_RFC authorization for billing for SAP CRM

3.2.16 Data Retention Tool Extended in SAP CRM

The Data Retention Tool Extended (DARTX) is used to periodically extract and retain tax-relevant data from selected SAP systems to support you in meeting legal data retention requirements for tax audit purposes. DARTX offers similar functions to the Data Retention Tool (DART) that is available in SAP ERP. DARTX differs from DART in that you can use it together with other SAP applications, for example SAP Customer Relationship Management (SAP CRM) or SAP GRC Global Trade Services. The standard delivery of DARTX includes a set of data segments and fields that can be used to help you fulfill tax audit requirements in Germany and the United States of America. The tool can be extended to meet similar requirements in other countries.

Why Is Security Necessary?

Security is necessary because DARTX accesses data in the SAP CRM system in the following areas:

- Billing

- Pricing
- Business transactions
- Business partners
- Taxes

Security Aspect of Dataflow and Processes

The figure below shows an overview of the data flow for the DARTX in SAP CRM.

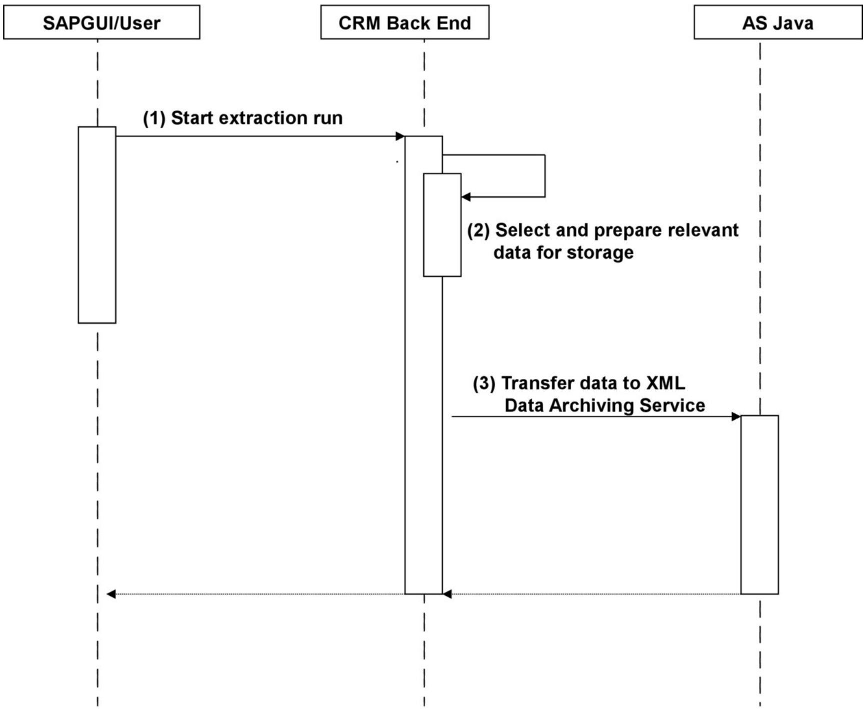

SAPGUI/User
CRM Back End
AS Java
(1) Start extraction run
(2) Select and prepare relevant data for storage
(3) Transfer data to XML Data Archiving Service

Figure 14: Overview of Process Steps for DARTX in SAP CRM

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

Table 201

Step	Description	Security Measure
1	Start extraction run	User Type: Dialog user
2	Select and prepare relevant data for storage	For more information, see the *Authorizations* section.
3	Transfer data to the XML Data Archiving Service	For more information, see the*Security Guide for XML DAS Archiving* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* : Search for *Security Guide for XML DAS Archiving*.

User Administration and Authentication

DARTX in SAP CRM uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP NetWeaver Application Server (SAP NetWeaver AS). 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 DARTX in SAP CRM.

User Management

User management for the billing component in SAP CRM uses the mechanisms provided by SAP NetWeaver AS ABAP, such as tools, user types, and password policies.

Table 202

Tool	Description
User and role administration with SAP NetWeaver AS: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction.	For more information, see User Administration and Authentication [page 18].

User Types

The following user types are required for DARTX in SAP CRM:

Table 203

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access billing transactions. Created by an SAP CRM system administrator.
SAP CRM	End user	No	System user	No	Mandatory user who can process background jobs.

Authorizations

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

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

Standard Roles

Table 204

Role	Role Description
`SAP_CRM_DARTX_INTERNAL_AUDITOR`	DARTX CRM

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by DARTX in SAP CRM:

Table 205

Authorization Object	Field	Description
`C_TXX_TF`	`ACTVT`	Generation of data extracts

Authorization Object	Field	Description
	BURKS	
C_TXX_TV	ACTVT BRGRU BURKS GJAHR	Generation of data views
C_TXX_TVC	ACTVT	Processing of data views

Network and Communication Security

The network topology for billing in SAP CRM is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM.

Communication Channel Security

The following table lists the various communication channels that are used between DARTX and other applications:

Table 206

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SAP CRM server to AS JAVA	HTTP/HTTPS	System ID, client name, host name, and all application data	System information and SAP CRM data

Data Storage Security

- For information on data storage security for DARTX, see the*Security Guide for XML DAS Archiving* in SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ◀: Search for *Security Guide for XML DAS Archiving*.
- For information on sources of information for XML-based data, see SAP Note 826000.

3.2.17 Rebates in SAP CRM

Why Is Security Necessary?

Security is necessary because the rebates component in SAP Customer Relationship Management (SAP CRM) does the following:

- Accesses data in the CRM system, such as business partner information in billing, and contains business information, such as invoices
- Has direct access to the tax engine and the pricing engine, where all products and prices are stored
- Is integrated with the Financial Accounting (FI) module of SAP ERP, which is important for financial services

User Administration and Authentication

The rebates component in SAP CRM uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 the rebates component in SAP CRM.

User Management

User management for the rebates component in SAP CRM uses the mechanisms provided by the SAP NetWeaver AS ABAP, such as tools, user types, and password policies. For an overview of how these mechanisms apply to the application, see the following sections:

Table 207

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information, see User Administration and Authentication [page 18].

User Types

The following users must be created for rebates in SAP CRM:

Table 208

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access rebates transactions. Created by an SAP CRM system administrator.
SAP CRM	N/A	No	System user	No	Mandatory user who can process background jobs.
SAP ERP	N/A	No	System user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, user can be a personal user or a system RFC user. Created by an SAP ERP system administrator.

Authorizations

The rebates component in SAP CRM uses the authorization provided by SAP NetWeaver Application Server (SAP NetWeaver AS). Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to this component.

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

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for rebate processing in ACE Customizing, because the rules in the SAP standard system are dummy rules. For more information, see the Access Control Engine [page 324] section.

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the rebates component in SAP CRM:

Table 209

Authorization Object	Field	Description
BEA_RDLH	ACTVT APPL BILL_ORG REB_PROF	Maintenance of the rebates due list
BEA_RPDH	ACTVT APPL BILL_ORG SETTL_TYPE	Creation and maintenance of rebate settlement documents
BEA_REXH	ACTVT APPL BILL_ORG EXTCT_TYPE	Creation and maintenance of rebate extracts
CRM_RBAG	ACTVT	Creation and maintenance of rebate agreements

Network and Communication Security

The network topology for the rebates component in SAP CRM is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to the rebates component.

Communication Channel Security

The following table lists the various communication channels that are used between the components of the rebates software and other applications:

Table 210

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
ERP server to CRM server	RFC	System ID, client, and host name, and all application data	System information and ERP data
CRM server to Internet Pricing and Configurator (IPC)	RFC	Pricing conditions	System information and CRM data
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data

The following figure illustrates the communication paths listed in the table above:

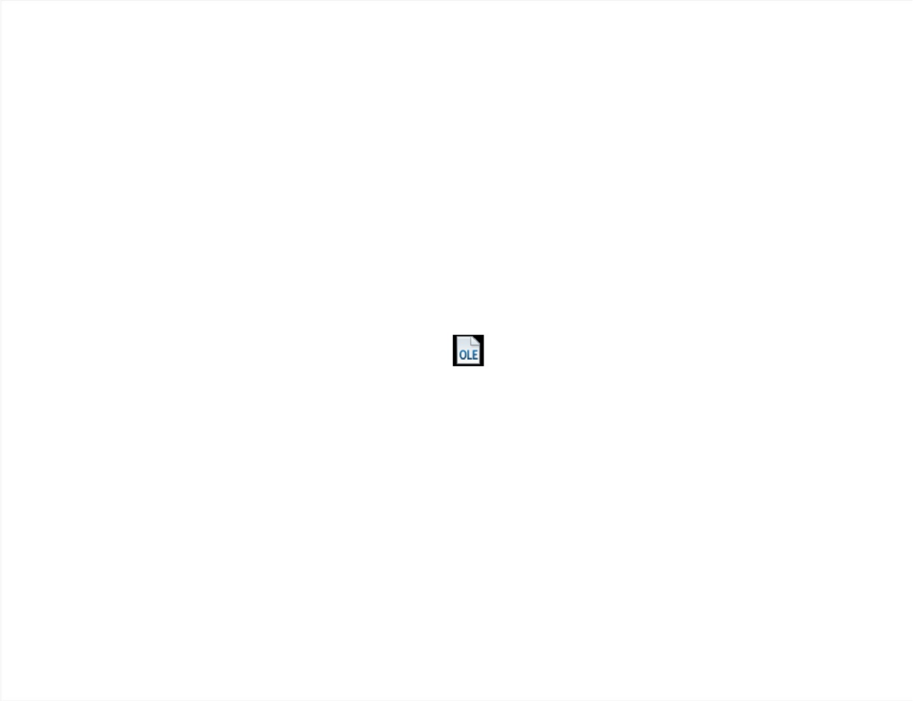


Figure 15: Communication Paths

In most cases, only application data is sent across (rebate extracts REXH/REXI/RCON and rebate settlement documents RPDH/RPDI).

The following data is received:

- Billing documents from the billing component in SAP CRM
- Rebate agreements from SAP CRM sales
- Status feedback from the FI module of SAP ERP

Important SAP Notes

Table 211

SAP Note Number	Short Text
1246837	S_RFC authorization for rebate processing in SAP CRM

3.2.18 Entitlement Management

Entitlement management is an ABAP-based application that allows you to create and track customer entitlements in SAP Customer Relationship Management (SAP CRM). Entitlement management is integrated with service parts management scenarios.

Entitlement management can post liabilities to financial accounting (FI) and controlling (CO) in SAP ERP by using the standard integration.

Why Is Security Necessary?

Security is necessary because entitlement management does the following:

- Accesses data in the SAP CRM system, such as business partner information or product information, and contains links to business information, such as invoices
- Has direct access to the pricing engine, where all products and prices are stored
- Is integrated with the FI module of SAP ERP

Security Aspect of Dataflow and Processes

The figure below shows an overview of the processes for the Entitlements Management in SAP CRM

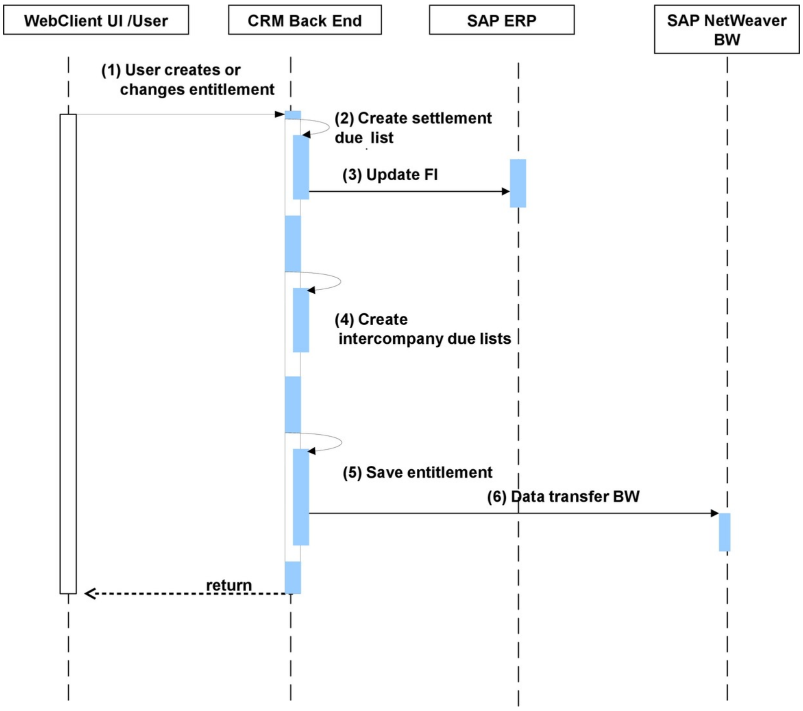


Figure 16: Overview of Process Steps for Entitlements Management

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

Table 212

Step	Description	Security Measure
1	User creates or changes an entitlement	User Type: Dialog user with assignment to business role and PFCG role, Communication Protocol, HTTP/HTTPS
2	System creates a new settlement due list (optional)	Not applicable
3	Newly created settlement due list on processing prepares for FI transfer	Asynchronous RFC based communication
4	New Intercompany due lists created (optional)	Not applicable
5	Entitlement is saved	Not applicable
6	Data transfer to BW	Asynchronous RFC based communication

Business Roles

The following business role for service parts management applies to entitlement management:

Table 213

Business Role	PFCG Role	Description
SPL	`SAP_CRM_UIU_SPL_PROFESSIONAL`	*CRM UIU Service Parts Logistics Management Professional*

The PFCG role `SAP_CRM_UIU_SPL_PROFESSIONAL` contains the role menu folder *SPL-ENT* with the menu items for entitlement management.

User Administration and Authentication

Entitlement management uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP NetWeaver Application Server (SAP NetWeaver AS). 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 the entitlement management application.

User Management

User management for entitlement management uses the mechanisms provided by SAP NetWeaver AS ABAP, such as tools, user types, and password policies. For an overview of how these mechanisms apply to the application, see the following sections:

Table 214

Tool	Description
User and role administration with SAP NetWeaver AS: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information, see User Administration and Authentication [page 18].

User Types

The following user types are required for entitlement management:

Table 215

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access entitlement management transactions. Created by an SAP CRM system administrator.
SAP CRM	End user	No	System user	No	Mandatory user who can process background jobs.
SAP ERP	End user	No	System user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the RFC destination, the user can be a personal user or a system RFC user. Created by an SAP ERP system administrator.
SAP BW	End User	No	System User	No	Mandatory user used for transferring data to SAP NetWeaver BW

Authorizations

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

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

Standard Authorization Objects

The following table shows the authorization objects for entitlement management:

Table 216

Authorization Object	Field	Description
/CEM/ALL	ACTVT /CEM/APPL /CEM/LE	Authorizations for entitlement management application
/CEM/DRP	ACTVT /CEM/PART /CEM/LE	Authorizations for entitlement management application for specific master data

Network and Communication Security

For information about the corresponding security recommendations, see Network and Communication Security [page 29].

Communication Channel Security

The following table lists the various communication channels that are used between the components of entitlement management and other applications:

Table 217

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data information, and customer data
CRM server to ERP server	RFC	System ID, client and host name, and all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client and host name, and all application data	System information and ERP data
CRM server to business intelligence (BI) server	RFC	System ID, client and host name, and all application data	System information and CRM data
CRM server to Internet Pricing and Configurator (IPC) (Necessary only if IPC runs on a separate installation. See SAP Note 855455)	RFC	Pricing conditions	System information and CRM data

In most cases, only application data is sent across (a neutral accounting document). The data that is received is status feedback from FI.

Important SAP Notes

Table 218

SAP Note Number	Short Text
1246838	S_RFC authorization for CRM Entitlement Management

3.2.19 SAP Incentive and Commission Management

SAP Incentive and Commission Management is an ABAP-based application that allows you to administer incentive management based on commission application in the ERP system from SAP Customer Relationship Management (SAP CRM).

SAP Incentive and Commission Management can post transaction data to case management in SAP ERP by using the standard integration.

Why Is Security Necessary?

Security is necessary because SAP Incentive and Commission Management does the following:

- Accesses business data in the CRM system, such as sales orders
- Accesses business intelligence (BI) data from the BI server
- Has direct access to ERP to post to commission management

Security Aspect of Dataflow and Processes

The figure below shows an overview of the processes for the Incentives and Commissions Management in SAP CRM.

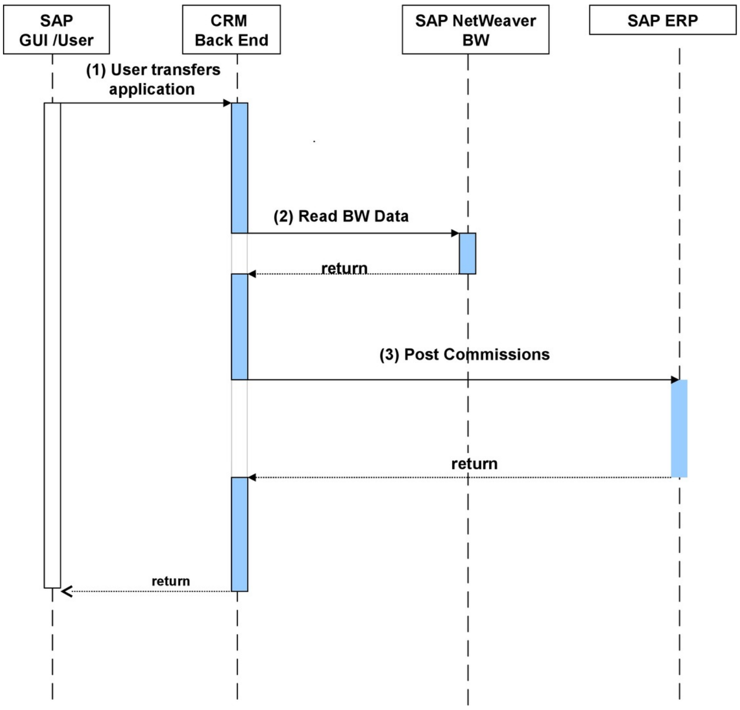


Figure 17: Overview of Process Steps for Incentives and Commissions Management in SAP CRM

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

Table 219

Step	Description	Security Measure
1	User initiates transfer application	User Type: Either dialog user or internet user with dialog user as alias

Step	Description	Security Measure
2	Read BW data (optional)	RFC based communication
3	Post commissions to SAP ERP	RFC based communication

User Administration and Authentication

SAP Incentive and Commission Management uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP NetWeaver Application Server (SAP NetWeaver AS). 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 the SAP Incentive and Commission Management application.

User Management

User management for SAP Incentive and Commission Management uses the mechanisms provided by SAP NetWeaver AS ABAP, such as tools, user types, and password policies. For an overview of how these mechanisms apply to the application, see the following sections:

Table 220

Tool	Description
User and role administration with SAP NetWeaver AS: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information, see User Administration and Authentication [page 18].

User Types

The following user types are required for SAP Incentive and Commission Management:

Table 221

System	User	Delivered?	Type	Default Password	Description
SAP CRM and SAP NetWeaver BW	End user	No	Dialog user	No	Mandatory user who can access SAP Incentive and Commission Management transactions and SAP NetWeaver BW. Created by an SAP CRM system administrator.
SAP CRM	End user	No	System user	No	Mandatory user who can process background jobs.
SAP ERP	End user	No	System user	No	Mandatory user used for data exchange between SAP CRM and SAP

System	User	Delivered?	Type	Default Password	Description
					ERP. Depending on the RFC destination, user can be a personal user or a system RFC user. Created by an SAP ERP system administrator.

Authorizations

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

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

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by SAP Incentive and Commission Management:

Table 222

Authorization Object	Field	Description
`CRMICM_APP`	`ACTVT`	Authorizations to execute CRM transfer application
`CRMICM_ALL`	`ACTVT`	All authorizations for the SAP Incentive and Commission Management application
`CRMICM_APL`	`ACTVT`	Authorizations to execute CRM transfer application

Network and Communication Security

The network topology for SAP Incentive and Commission Management is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM.

Communication Channel Security

The following table lists the various communication channels that are used between the components of SAP Incentive and Commission Management and other applications:

Table 223

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to ERP server	RFC	System ID, client, host name, and all application data	System information and CRM data

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to BI	RFC	System ID, client, host name, and all application data	System information and BI data

In most cases, only application data is sent (for example, sales information). The following data is received:

- Status feedback from commissions management in SAP ERP
- BI data from BI

Important SAP Notes

Table 224

SAP Note Number	Short Text
1248401	S_RFC authorization for CRM Incentives and Commission Mgmt

3.2.20 Pipeline Performance Management

Pipeline Performance Management (PPM) is part of SAP Customer Relationship Management (CRM), and works hand in hand with opportunity management. PPM is an interactive application that helps sales managers and sales representatives to do the following:

- Analyze their sales pipeline using different reports
- Identify gaps and critical opportunities
- Identify and monitor opportunity changes in the pipeline
- Simulate what-if scenarios
- Promptly trigger the correct actions to resolve issues and to meet their targets

User Management and Authentication

PPM uses the user management and authentication mechanisms of SAP NetWeaver; in particular, the security features of SAP NetWeaver Application Server (SAP NetWeaver AS) and of the standard WebClient UI framework. 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 PPM.

User Management

Table 225

Tool	Description
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information about user and role administration, see Business Roles [page 17] and User Administration and Authentication [page 18].

User Types

The following users must be created for PPM:

Table 226

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access PPM Customizing and the PPM application. Created by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user for communication with the ERP server for response messages from SAP ERP. Created by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	The same RFC destination is used to communicate from SAP NetWeaver Business Warehouse (SAP NetWeaver BW) as with the other SAP CRM business objects. The user in the SAP CRM system who handles the requests from SAP NetWeaver BW to transfer data (user ALEREMOTE) needs to have two specific authorization objects: `CRM_ORD_LP` and `S_USER_GRP`. SAP NetWeaver BW authorization management enforces proper authorization for SAP NetWeaver BW data so that users only see data for which they are authorized. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *SAP NetWeaver Business Warehouse*.

Authorizations and Delivered Security Features

PPM is delivered with the following:

- Job roles
  - *Sales Representative*
  - *Sales Manager*

  The PPM application uses multiple authorization objects, but only one is PPM-specific: `CRM_PPM`. This object allows users to set authorizations for three PPM applications (activities): quota planning, options page, and churn rates. Since these applications are accessible only to sales managers, the `CRM_PPM` settings do not affect sales representatives. It is sufficient for the sales representative to be assigned to a business role that has standard authorizations set up, regardless of `CRM_PPM`. PPM differentiates between sales representatives and sales managers based on the organizational model assignment, and not based on the authorizations. Therefore, no additional setup is required for sales representatives with regard to the PPM authorization object.

i Note

The following points describe the setup for the PPM-specific authorization object and therefore only apply to the *Sales Manager* role.

Business role

Since PPM is a sales application, it uses a sales business role.

Table 227

Business Role	PFCG Role	Description
SLS-PRO	SAP_CRM_UIU_SLS_PROFESSIONAL	Sales Professional

Authorization object

Table 228

Authorization Object	Description
CRM_PPM	Authorization Object for Pipeline Performance Management

CRM_PPM

The PPM authorization object CRM_PPM encompasses the following parameters:

Table 229

Field Text	Field Name	Values
OrgUnitID	ORGUNITID	If you enter an asterisk (*), you have authorization for all organizational units. If you enter a range (*From* and *To*) or a single organizational unit, you restrict the authorization to those specific organizational units.
Process Type in PPM	PROCTYPE	If you check the following activities, they are activated for the authorization profile: ● Churn Rates in PPM (PPMCHUR) ● Options in PPM (PPMOPTI) ● Quota Planning in PPM (PPMQUOP)
Activity	ACTVT	If the *Change* value is checked, you have authorization to edit. Otherwise, you only have display rights.

- Authorization proposal

  An authorization proposal is available in the standard system for all PPM-related UIU_COMP components. You can view this authorization proposal using the profile generator (PFCG) transaction in the generated authorization profile.

  Entries maintained in the proposal provide minimal authorizations by default. You must maintain them in a customer namespace to give further rights to the PFCG role (using transactions SU24 and SU25).

For more information about these authorization objects, see the *Maintain the Authorization ObjectsSU22* transaction and double-click the authorization object.

Communication Channel Security

The communication channel used is ABAP SQL for the connection to the database.

Network Security

Pipeline Performance Management is based on SAP NetWeaver platform and middleware in SAP CRM. For more information about the applicable security guidelines and recommendations, see the SAP NetWeaver Security Guide and the corresponding section of Component-Specific Guidelines: SAP CRM [page 68], and Network and Communication Security [page 29].

Communication Destinations

The PPM application uses the following framework:

1. Interaction Center Web Client (IC WebClient) UI framework
2. One Order Framework (including Reporting Framework)

Consequently the underlying communication destinations and channels are used.

3.3 Service

Service processing in SAP Customer Relationship Management (SAP CRM) includes functions in the following areas:

- Service core

  The functions in this area enable you to manage your service cycle, starting with managing service contracts and warranties, through to processing service order quotations and service orders, complaints and returns, and service confirmations.

- IT service management

  The functions in this area enable you to organize and manage information pertaining to information technology (IT) service support and delivery within your company. In addition to tracking and resolving issues within the IT infrastructure, you can measure and evaluate the quality of services provided.

In both areas, service analytics functions support you in analyzing the success of your operations from diverse perspectives.

Security Aspects of Data Flow and Processes

The following figure shows the data flow in service order processing. With the exception of steps *Credit Check* and *Availability Check*, the figure also applies to other service transactions.

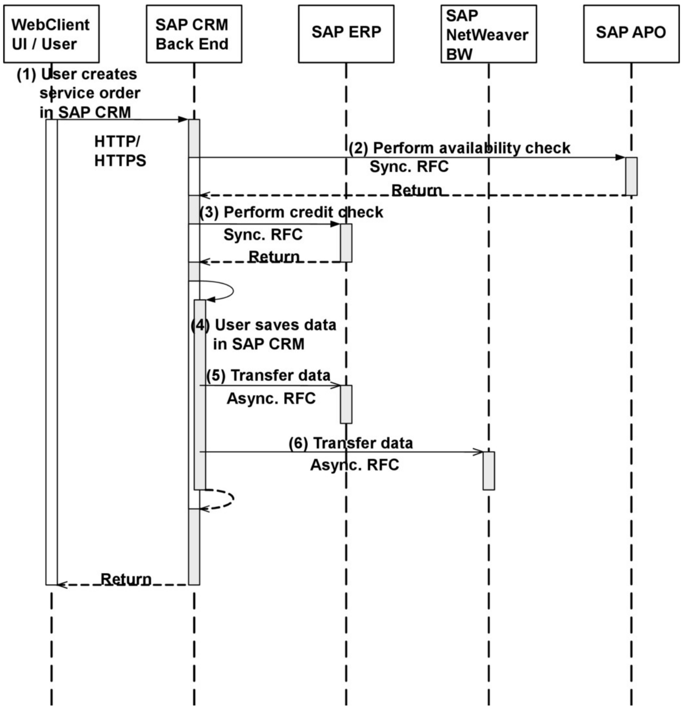


Figure 18: Overview of Process Steps for Service Order Processing

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

Table 230

Step	Description	Security Measure
1	User creates service order in SAP CRM	• User type: Dialog user with assignment to business role `SERVICEPRO` and corresponding PFCG role • Communication protocol HTTP/ HTTPS
2	Perform availability check (relevant for sales items and service part items only)	Not applicable (synchronous RFC)
3	Perform credit check	Not applicable (synchronous RFC)
4	User saves data in SAP CRM	Not applicable
5	Transfer data to SAP ERP	• Not applicable (synchronous RFC) • If payment cards are used, see section Payment Card Security According to PCI-DSS [page 42].
6	Transfer data to SAP NetWeaver BW	Not applicable (synchronous RFC)

Business Roles

Table 231

Business Role	PFCG Role	Description
SERVICEPRO	SAP_CRM_UIU_SRV_PROFESSIONAL	Service Professional
ITSERVICEPRO	SAP_CRM_UIU_SRQM_PROFESSIONAL	IT Service Professional
ITSERVREQU	SAP_CRM_UIU_SRQM_REQUESTER	IT Service Requester

User Administration and Authentication

User Management

Table 232

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialog user	No	Obligatory user who can access service transactions. To be maintained by an SAP CRM system administrator.
SAP NetWeaver Business Warehouse (SAP NetWeaver BW)	Personal user	No	Dialog user	No	Obligatory user who can access SAP NetWeaver BW applications. To be maintained by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Obligatory user who can process background tasks. To be maintained by an SAP CRM system administrator.
SAP ERP	Personal or technical user	No	Dialog or system user	No	Obligatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, user can be a personal user or a system RFC user. To be maintained by an SAP ERP system administrator.
SAP Supplier Chain Management (SAP SCM) – SAP Advanced Planning &	Personal or technical user	No	Service user	No	Obligatory user for data exchange between SAP CRM and SAP SCM.

System	User	Delivered?	Type	Default Password	Description
Optimization (SAP APO)					
SAP Supply Network Collaboration (SAP SNC)	Personal user	No	Dialog user	No	Obligatory user for SAP SNC

User Management Tools

Table 233

Tool	Description
User Maintenance (`SU01`) transaction	For more information, see User Administration and Authentication [page 18].

User Types

The personal user type is used to create users such as the following:

- Dialog users
- Background users

Customers must create the following users:

- Individual users to use with the standard processes that are delivered
- Initial identification parameters, such as the password and certificate for the users

> Note
>
> This is not done by SAP.

Network and Communication Security

The network topology for enterprise service and analytics is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and Component-Specific Guidelines: SAP CRM [page 68] also apply to enterprise service and analytics.

Communication Channel Security

The following communication channels are used:

- Remote function call (RFC)
- Business document (BDoc) type: `BUS_TRANS_MSG` and `COUNTER`
- ABAP Structured Query Language (SQL) for the connection to database

Communication Destinations

Table 234

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client, and host name, and all application data	System information and ERP data
CRM server to BI server	RFC	System ID, client, and host name, and all application data	System information and CRM data
CRM server to Internet Pricing and Configurator (IPC) (Necessary only if IPC runs on a separate installation; See SAP Note 855455.)	RFC	Pricing conditions	System information and CRM data
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data
SAP CRM to SAP Supply Chain Management (SAP SCM) – SAP APO	RFC	Application data	Password and user for SCM – APO required
SAP CRM to SAP SNC (SCM server)	HTTP/HTTPS	Application	Password and user for SAP SNC required

3.3.1 Service Core

With the core service functions, you can manage your service cycle, starting with managing service contracts and warranties, through to processing service order quotations and service orders, complaints and returns, and service confirmations.

Business Roles

For all core service transactions, that is, service transactions not belonging to IT service management, the *Service Professional* business role is relevant:

Table 235

Business Role	PFCG Role	Description
SERVICEPRO	SAP_CRM_UIU_SRV_PROFESSIONAL	*Service Professional*

Authorizations

The following authorization objects and authorization fields are used:

Table 236

Authorization Object	Authorization Field
CRM_CO_SE (Business object service contract)	ACTVT
CRM_CON_SE (Business object service confirmation)	ACTVT
CRM_CO_BR (Business object billing request)	ACTVT
CRM_CLM (Business object warranty claim)	ACTVT
CRM_OUTL (Business object outline agreement)	ACTVT
CRM_ORD_LP (Visibility in organization model)	CHECK_LEV (Scope of processed objects) PR_TYPE (Transaction type) ACTVT
CRM_ORD_OE (Allowed organizational units)	SALES_ORG (Sales organization) SERVICE_OR (Service organization) DIS_CHANNE (Distribution channel) SALES_ORG (Sales office) SALES_GROU (Sales group) ACTVT
CRM_ORD_OP (Own documents)	PARTN_FCT (Partner function) PARTN_FCTT (Partner function category) ACTVT
CRM_ORD_PR (Business transaction type)	PR_TYPE (Transaction type) ACTVT
CRM_TXT_ID (Text ID)	TEXTOBJECT (Texts: application object) TEXTID (Text ID) ACTVT
CRM_SEO (Business object service order)	ACTVT
CRM_ORD_PC	ACTVT PR_TYPE (Transaction type)
CRM_CMP (Business object complaint)	ACTVT

Authorization Object	Authorization Field
S_SCMG_CAS (Case management)	CASETYPE (Case type) SCMG_ACT (Activity) SCMG_KEY (Dynamic key for case) SCMG_LVL (Authorization level) SCMG_ROLE (Role of user) SPS_ID (Element kind ID)
CRM_SFC (Simple field check)	ACTVT LEVEL1 (Authorization level)
CRM_CATEGO (Multilevel categorization)	ACTVT ASP_STATE (Schema status) LN_TYPE (Object links) SC_ID (Application ID) SC_PART (Part)
S_TCODE (Transaction code check at transaction start)	TCD (IC_LTX authorization value)

RFC Authorizations for Authorization Object S_RFC: CRM to ERP

Table 237

RFC_TYPE	RFC_NAME	ACTVT
FUGR	CRM_CO_SLS	16
FUGR	KEC1CRMCOPASALES	16
FUGR	CRMA	16
FUGR	/SPE/CRM_RET_LOG	16
FUGR	FILA	16
FUGR	/SPE/CRM_EXECUTION	16
FUGR	CRM_SERV_CONFIRM_PROXIES	16
FUGR	CRM_SRV_LOG_EXT CRM	16
FUGR	CRM_SRV_LOG	16
FUGR	CRM_QM_NOTIF	16
FUGR	LATP	16

RFC Authorizations for Authorization Object S_RFC: ERP to CRM

Table 238

RFC_TYPE	RFC_NAME	ACTVT
FUGR	SMOUTIL	16

RFC Authorizations for Authorization Object S_RFC: CRM to APO

Table 239

RFC_TYPE	RFC_NAME	ACTVT
FUGR	10400	16

Authorizations for Advanced Returns Management

The following table lists the RFC authorizations for authorization object S_RFC — CRM to ERP:

Table 240

RFC_TYPE	RFC_NAME	ACTVT
FUGR	ERP_LORD	16
FUGR	MSR_TRC_UI	16
FUGR	ERP_SALES_O2C_BIL	16

The following table lists the RFC authorizations for authorization object S_RFC — CRM to APO:

Table 241

RFC_TYPE	RFC_NAME	ACTVT
FUGR	/SAPAPO/ATPR	16
FUGR	10400	16

The following table lists the required authorizations for downloading Customizing data from the SAP ERP system to the SAP CRM system:

Table 242

System	Authorization Object	Authorization Field	Authorizations Value	Comment
SAP CRM	CMW_CRMADP	ACTVT	16	Not applicable
SAP ERP	SCRMMW	MW_ACT	1	Assign this authorization to the user defined in the RFC destination for the target SAP ERP system.
SAP ERP	SCRMMW	MW_ACT	6	Assign this authorization to the user defined in the RFC destination for the target SAP ERP system.

3.3.2 Incident Management

In IT service management, the aim of incident management is to restore normal service operation as soon as possible after a breakdown while minimizing the disturbance to business operations. Incident management allows customers or employees (*IT Service Requester* role) to contact the service desk (*IT Service Professional* role) when their IT-related devices or services are not working properly, or when requesting a service.

Business Roles

Table 243

Business Role	PFCG Role	Description
ITSERVICEPRO	SAP_CRM_UIU_SRQM_PROFESSIONAL	IT Service Professional
ITSERVREQU	SAP_CRM_UIU_SRQM_REQUESTER	IT Service Requester

User Management and Authentication

Incident management uses the normal user management of SAP NetWeaver and requires dialog users:

Table 244

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Authorizations

Several authorization objects exist, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 245

Authorization Object	Description
CRM_CATEGO	Authorization Object for Coherent Categorization
CRM_IBASE	Authorization Object Installed Base
CRM_INCDNT	Authorization Object CRM Order: Incident Management
CRM_CHKLST	Authorization Object CRM ITSM Checklist
CRM_ORD_LP	Authorization Object CRM Order - Visibility in Org. Model
CRM_ORD_OE	Authorization Object CRM Order - Allowed Organ. Units
CRM_ORD_OP	Authorization Object CRM Order - Own Documents
CRM_ORD_PR	Authorization Object CRM Order - Business Transaction Type
CRM_TERRMA	Territory Management
CRM_TXT_ID	CRM: Text ID
S_TCODE	Transaction Code Check at Transaction Start

Authorizations for the IT Service Professional Business Role

The standard business role *IT Service Professional* can create, modify, search, and delete incidents.

Maintain the authorization objects as follows under the *IT Service Professional* role:

Table 246

Authorization Object	Authorization Fields	Authorization Values
CRM_ORD_LP	ACTVT	Full Access
CRM_ORD_OE	ACTVT	Full Access
S_RFC	ACTVT RFC_NAME RFC_TYPE	16 CRM_SRV_SOLMANINT_WS FUGR
S_TCODE	TCD	IC_LTX

Authorizations for the IT Service Requester Role

The standard business role *IT Service Requester* can only create and search for incidents and knowledge articles. Problems and requests for change are not available to this business role.

Maintain the authorization objects as follows under the *IT Service Requester* role:

Table 247

Authorization Object	Authorization Fields	Authorization Values
CRM_ORD_LP	ACTVT	No Access
CRM_ORD_OE	ACTVT	No Access
S_RFC	ACTVT RFC_NAME RFC_TYPE	16 CRM_SRV_SOLMANINT_WS FUGR
S_TCODE	TCD	IC_LTX

Checklist

Table 248

Feature	Check	How to Check
Change an incident or some of its properties	User settings for the incident authorization objects	If you are not authorized to perform changes, the system rejects your changes.
For the *IT Service Requester* role, only the user's own documents can be seen in the incident search results.	User settings for the authorization objects CRM_ORD_LP and CRM_ORD_OE have been maintained properly	If the authorization is set up correctly, only the user's own documents are visible in the incident search results.
For the *IT Service Professional* role, all documents appear in the incident search results.	User settings for the authorization objects CRM_ORD_LP and CRM_ORD_OE have been maintained properly	If the authorization is set up correctly, all documents are visible in the incident search results.

3.3.3 Problem Management

In IT service management, the aim of problem management is to minimize the adverse effects of problems and breakdowns in business operations by actively preventing errors, problems, and breakdowns, and by quickly and effectively resolving any problems that do occur.

Business Roles

For problem management only the *IT Service Professional* role is delivered:

Table 249

Business Role	PFCG Role	Description
ITSERVICEPRO	SAP_CRM_UIU_SRQM_PROFESSIONAL	IT Service Professional

User Management and Authentication

Problem management uses the normal user management of SAP NetWeaver and requires dialog users:

Users

Table 250

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 251

Authorization Object	Description
CRM_CATEGO	Authorization Object for Coherent Categorization
CRM_IBASE	Authorization Object Installed Base
CRM_INCDNT	Authorization Object CRM Order: Incident Management
CRM_CHKLST	Authorization Object CRM ITSM Checklist
CRM_ORD_LP	Authorization Object CRM Order - Visibility in Org. Model
CRM_ORD_OE	Authorization Object CRM Order - Allowed Organ. Units
CRM_ORD_OP	Authorization Object CRM Order - Own Documents
CRM_ORD_PR	Authorization Object CRM Order - Business Transaction Type
CRM_TERRMA	Territory Management
CRM_TXT_ID	CRM: Text ID

Authorization Object	Description
S_TCODE	Transaction Code Check at Transaction Start

Authorizations for the IT Service Professional Business Role

The standard business role *IT Service Professional* can create, modify, search, and delete problems.

Maintain the following authorization objects for the *IT Service Professional* role:

Table 252

Authorization Object	Authorization Fields	Authorization Values
CRM_ORD_LP	ACTVT	Full Access
CRM_ORD_OE	ACTVT	Full Access
S_RFC	ACTVT RFC_NAME RFC_TYPE	16 CRM_SRV_SOLMANINT_WS FUGR
S_TCODE	TCD	IC_LTX

Checklist

Table 253

Feature	Check	How to Check
Change a problem or some of its properties	User settings for the problem authorization objects	If you are not authorized to perform changes, the system rejects your changes.
For the *IT Service Professional* role, all documents appear in the problem search results.	User settings for the authorization objects CRM_ORD_LP and CRM_ORD_OE have been maintained properly.	If the authorization is set up correctly, all documents are visible in the problem search results.

3.3.4 Requests for Change

In IT service management, the goal of requests for change (RfC) is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes. This minimizes the impact of change-related incidents upon service quality, and consequently improves the day-to-day operations of the organization.

Business Roles

For RfCs, the *IT Service Professional* role is relevant:

Table 254

Business Role	PFCG Role	Description
ITSERVICEPRO	SAP_CRM_UIU_SRQM_PROFESSIONAL	IT Service Professional

User Management and Authentication

RfCs use the normal user management of SAP NetWeaver and require dialog users.

Users

Table 255

System	User	Delivered?	Type	Default Password
SAP Customer Relationship Management (SAP CRM)	Normal user	No	Dialog user	Arbitrary

Authorization Objects

Several authorization objects exist, allowing for specific authorizations involving the employee responsible as a central entity. These authorization objects include the following:

Table 256

Authorization Object	Description
CRM_APPRVL	Authorization Object for Approval Process
CRM_CATEGO	Authorization Object for Coherent Categorization
CRM_IBASE	Authorization Object Installed Base
CRM_INCDNT	Authorization Object CRM Order: Incident Management
CRM_CHKLST	Authorization Object CRM ITSM Checklist
CRM_ORD_LP	Authorization Object CRM Order - Visibility in Org. Model
CRM_ORD_OE	Authorization Object CRM Order - Allowed Organ. Units
CRM_ORD_OP	Authorization Object CRM Order - Own Documents
CRM_ORD_PR	Authorization Object CRM Order - Business Transaction Type
CRM_TERRMA	Territory Management
CRM_TXT_ID	CRM: Text ID
S_TCODE	Transaction Code Check at Transaction Start

Authorizations for the IT Service Professional Role

The standard business role *IT Service Professional* can create, modify, search, and delete RfCs.

Maintain the authorization objects for the *IT Service Professional* role as follows:

Table 257

Authorization Object	Authorization Fields	Authorization Values
CRM_ORD_LP	ACTVT	Full Access
CRM_ORD_OE	ACTVT	Full Access
S_RFC	ACTVT	16 CRM_SRV_SOLMANINT_WS

Authorization Object	Authorization Fields	Authorization Values
	RFC_NAME RFC_TYPE	FUGR
S_TCODE	TCD	IC_LTX

Approval Processes

Before an RfC can be planned and tested, it first needs to be approved by one or several parties to minimize any negative effects to the infrastructure.

For each RfC, its approval process is implemented as an approval procedure that contains approval steps (which are approved by the responsible parties). To control access rights to display, create, change, or delete an approval procedure or approval step, use the following authorization object:

Table 258

Authorization Object	Field	Value
CRM_APPRVL	ACTVT	Full Access

Checklist

Table 259

Feature	Check	How to Check
Change an RfC or some of its properties	User settings for the RfC authorization objects	If you are not authorized to perform changes, the system rejects your changes.
For the *IT Service Professional* role, all documents appear in the RfC search results.	User settings for the authorization objects CRM_ORD_LP and CRM_ORD_OE have been maintained properly	If the authorization is set up correctly, all documents are visible in the RfC search results.

3.4 CRM via E-Mail

For e-mail communication to meet the highest level of security standards, digital certificates and encryption should be used to transmit e-mails. To meet legal requirements in some countries, it is mandatory to use encrypted and digitally signed e-mails to transmit sensitive data.

CRM via E-Mail is based on the E-Mail Response Management System (ERMS) application in the Interaction Center (IC) scenario and SAP Netweaver. Therefore, the corresponding security guides also apply to CRM via E-Mail.

Important SAP Notes

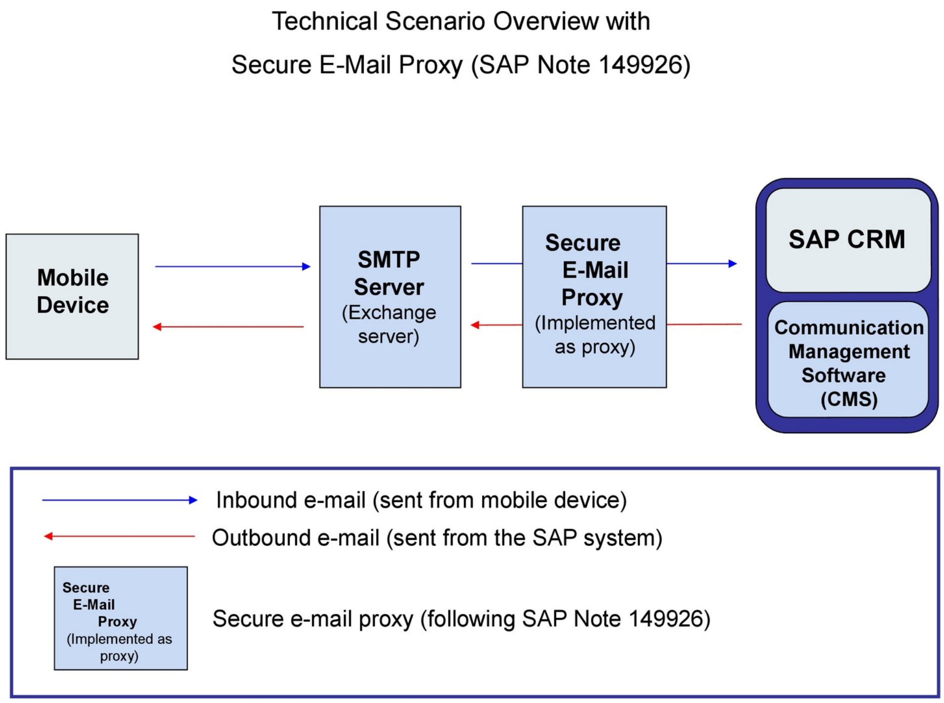
The following table shows the most important SAP Notes that apply to the security of CRM via E-Mail (CRM-BF-E2C):

Table 260

SAP Note Number	Title	Comment
149926	Secure e-mail: Encryption, digital signature	This note is mandatory for secure use of CRM via E-Mail.

Technical Landscape

The figure below shows an overview of the technical system landscape for CRM via E-Mail. This is one of the possible landscapes and may vary based on the third party e-mail security product chosen by the customer.


Technical Scenario Overview with

Secure E-Mail Proxy (SAP Note 149926)

Mobile Device
SMTP Server (Exchange server)
Secure E-Mail Proxy (Implemented as proxy)
SAP CRM
Communication Management Software (CMS)
Inbound e-mail (sent from mobile device)
Outbound e-mail (sent from the SAP system)
Secure E-Mail Proxy (Implemented as proxy)
Secure e-mail proxy (following SAP Note 149926)

Figure 19: Technical System Landscape for SAP CRM via E-Mail

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *Function-Oriented View* : Search for *SAPconnect (BC-SRV-COM)*.

User Administration and Authentication

CRM via E-Mail uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver 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 CRM via E-Mail.

User Management Tools

The following table shows the tools to use for user management and user administration with CRM via E-Mail.

Table 261

Tool	Description	Prerequisites
Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *CRM via E-Mail* ◀	For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security* › *Identity Management* ◀.	Each user who is authorized to use CRM via E-Mail must be mapped to an employee maintained in CRM Master Data. The e-mail address that the user uses to send e-mails must be maintained in the Employee Master Data.
Maintain User Profile (transaction `SU01`)	For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security* › *Identity Management* ◀.	N/A

Authentication

Each user who is authorized to use CRM via E-Mail must be mapped to an employee maintained in CRM Master Data. The e-mail address that the user uses to send e-mails must be maintained in the Employee Master Data.

To determine if the e-mail is authentic, digital signatures must be used.

Each CRM via E-Mail user must send digitally signed e-mails from an e-mail account with an e-mail id (address) that matches the e-mail id maintained in the employee master data record on the CRM Server.

A third party e-mail security product authenticates the digital signature of the e-mail. The third party product puts an indicator on the incoming e-mail to show whether the digital signature is valid. This indicator can be programmatically verified in the security Business Add-In (BAdI) provided by the CRM via E-Mail application. If the digital signature is found to be invalid or not present, the e-mail is not processed by the application.

Standard Users

The following table shows the standard users that are necessary for operating CRM via E-Mail (`CRM-BF-E2C`). This user is not delivered but has to be created:

Table 262

User ID	Type	Password	Description
E2C	Service user	N/A	The user used to receive e-mails in the system. The e-mail address that receives the e-mails should be specified in the user details.

Authorizations

CRM via E-Mail uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Security Guide* also apply to CRM via E-Mail.

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role administration, use the Profile Generator (transaction PFCG) when using ABAP technology, and the user management engine's user administration console when using Java.

CRM via E-Mail uses an additional level of authorizations that are handled in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *CRM via E-Mail* ◀. Authorizations can be given based on the user (employee) or based on the role. Authorizations based on the user override the authorizations based on role. For example, a particular CRM via E-Mail service has given authorizations to all users with the role *Channel Manager*. If a particular user is not assigned to the role *Channel Manager*, they can still be given authorization to use the service based on the user (employee) in the system.

Communication Channel Security

The following table shows the communication channels used by CRM via E-Mail (CRM-BF-E2C), the protocol used for the connection, and the type of data transferred.

Table 263

Communication Channel	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
E-Mail	SMTP	All application data	Depending on the legal requirements of the country that the customer is operating in, certain data may be marked as sensitive.

Note

E-mails should be digitally signed and encrypted when using CRM via E-Mail to achieve the highest level of security. The default security BAdI does not allow insecure e-mails. Customers are required to implement this BAdI based on the third party e-mail security product used for e-mail encryption and digital signature.

3.5 Further Topics

Displaying Workflows for Business Objects

The WebClient UI component GSWIOBJREL can be used in overview pages to display a simplified log of workflows that are related to the business object that is currently displayed.

Why is Security Necessary?

The current user can view a simplified workflow log in the WebClient UI component GSWIOBJREL.Be aware that implementing this feature provides the user with information that was not previously visible in the WebClient UI.

Important SAP Notes

The most important SAP Note that applies to the security of the WebClient UI component GSWIOBJREL is found in the following table.

Table 264

Title	SAP Note	Comment
Integration of UI Component GSWIOBJREL	1717812	This note describes how GSWIOBJREL can be integrated with the WebClient UI components and overview pages. It also describes the security-relevant aspects for customers, using CRM 7.0 EHP1 or CRM 7.0 EHP2. It will be updated if new security-relevant aspects of GSWIOBJREL are identified in the future.

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

Authorizations

The WebClient UI component GSWIOBJREL does not provide any filtering mechanism, such as an authorization check to restrict the workflows or workflow tasks that are shown to the user.

To restrict the information that can be seen by the user, you must use the mechanisms provided generically by the SAP Business Workflow or the WebClient UI framework. For example: You can only integrate the new UI block of GSWIOBJREL for dedicated business roles.

You can also observe the authorizations you granted for transaction CRMD_ORDER here, since this transaction shows the simplified workflow log in the SAP GUI.

Integration of Social Collaboration with SAP CRM

SAP Jam content is available to you on various overview pages for several business objects and on the homepage for the CRM WebClient UI.

Why is Security Necessary?

The integration of social collaboration with SAP CRM raises multiple aspects that may be relevant to the security of your CRM system. For example:

- Which data can be seen or modified by SAP Jam users?
- Which data can be seen or modified by SAP CRM users?
- Which data is stored in SAP CRM and which data is stored in SAP Jam?
- What about network and communication security when connecting SAP CRM and a social collaboration application?

If you are using the add-on *Provide OData Services for the Integration of SAP Jam with SAP CRM Using Gateway 1.0 (CRMSWI01)* for the social collaboration with SAP CRM based on SAP NetWeaver Gateway, SAP CRM data is transferred to the social collaboration application.

The section *Security Aspects of Data, Data Flow, and Processes* describes how this can be limited to specific SAP CRM business object types.

We provide this security guide to assist you in securing your SAP CRM installation.

Before You Start

- Fundamental Security Guides

When integrating social collaboration with SAP CRM you should refer to the security information about SAP Jam that is available on request.

When using the add-on CRMSWI01 you should also refer to the SAP NetWeaver Gateway Security Guide at help.sap.com/nwgateway#section4 > *Security Guide*.

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

- Important SAP Notes

  The most important SAP Notes that apply to the security of the integration of social collaboration with SAP CRM are shown in the following table:

Table 265

Title	SAP Note	Comment
StreamWork: Security Aspects of the ABAP Integration Library	1670669	This note lists the constraints regarding security and data privacy that have to be considered when using the SAP Social Media ABAP Integration Library (SAIL).
Social Media Integration with SAP CRM: Security Aspects	1766499	This note contains information about security aspects of the social media integration with SAP CRM.
Customizing Guide: Business Object Change	1797033	This note is relevant if you are using the add-on CRMSWI01

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

- Configuration

  Refer to the following documents, since correct configuration is important for the security of the integration of social collaboration with SAP CRM:

  - *SAP StreamWork ABAP Integration – Configuration Guide* at scn.sap.com/docs/DOC-24691
  - Business Functions in SAP NetWeaver: *Enable Social Media ABAP Integration 3* [external document]

When using the add-on CRMSWI01, see also:

- SAP NetWeaver Gateway Configuration Guide at help.sap.com/nwgateway#section4 > *Configuration Guide*.
- The release note for the add-on CRMSWI01. Choose transaction SFW5 and then the business function CRM_SWI_GW. The release note *SAP CRM BO Change Notification Using SAP NetWeaver Gateway* is linked to the business function. Or see help.sap.com/crm -> *Release Notes*.

Security Aspects of Data, Data Flow, and Processes

The integration of social collaboration with SAP CRM introduces new processes providing SAP CRM users with the option of seeing, creating, and modifying data stored in a social collaboration application.

All data that is shown or can be created or modified in the WebClient UI views of SAP CRM for the social collaboration integration is stored on the social collaboration application. No data is stored in CRM database tables.

To ensure that your data flow between the social collaboration application and SAP CRM is secure, see the configuration guide for SAP Social Media ABAP Integration Library. For more information, see the chapter “Configuration” .

The link between CRM business objects, such as the individual account or sales quotation and SAP Jam groups is implemented by the SAP Social Media ABAP Integration Library (SAIL). SAIL stores the link in a database table in the SAP NetWeaver system (CRM System).

A similar link exists between the CRM business object and the SAP Jam topic object stored by SAIL.

Some social collaboration applications provide a feature that you can use to send e-mail notifications to users. Since e-mails are usually sent in an unsecure fashion using the Internet, you should be aware that such e-mails could contain business data if the CRM user has used information from a SAP CRM business object for the collaboration.

Example:

A SAP CRM user might create a SAP Jam group that is related to a SAP CRM opportunity and use the opportunity name as the name for the new SAP Jam group.In this case, an e-mail notification about changes to the SAP Jam group will contain the text that was originally used as name of the SAP CRM opportunity.

We recommend switching off the e-mail notifications in your social collaboration application when using the integration of social collaboration with SAP CRM.

Security information about SAP Jam is available on request.

If you use the add-on CRMSWI01, be aware that business object data from SAP CRM is transferred to SAP Jam using the notifications mechanism of SAP NetWeaver Gateway if an SAP CRM business object is changed. Such notifications are sent for several types of SAP CRM business objects. A dedicated OData service is available for each of these business object types. You can enable and disable the notifications for each business object type by enabling or/ disabling the related OData service in Customizing for your SAP NetWeaver Gateway server under *Application Server* > *Basis Services* > *Collaboration* > *Gateway Notifications* > *Activate OData Service for Notification*.

For more information, see SAP Note 1797033.

User Administration and Authentication

SAP CRM uses the user management and authentication mechanisms provided with the SAP NetWeaver platform in particular the SAP NetWeaver Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide* apply to the user authentication of the SAP CRM users for the social collaboration integration scenario. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide*.

The e-mail address is used to map the SAP CRM user to the social collaboration application user: The e-mail addresses for the SAP CRM user and the SAP Jam user have to be identical.

If you are using the add-on CRMSWI01, be aware that every SAP CRM user who changes a business object (known as an actor) also needs an SAP Jam user account to have the business object change notification published via SAP Jam and SAP NetWeaver Gateway. The Social Media ABAP Integration Library repersonalizes Gateway notifications from the technical Gateway user to the original actor. This is obligatory, since SAP Jam does not allow feed entries to be pushed on behalf of other users.

Authorizations

The authorization to view, create, or modify data or to make information accessible to other users in SAP Jam is mainly controlled by the privacy settings of the SAP Jam group to which the data belongs.

If an SAP CRM user assigns information from an SAP CRM business object, such as an individual account to an SAP Jam group, this information is no longer secured by the SAP CRM authorization mechanisms, and is instead subject to the authorization concept of the social collaboration application.

From a security perspective, this is equivalent to copying information from the SAP CRM system to the social collaboration application system using the user's client operation system.

If you are using the add-on CRMSWI01 you should consider that business object data from SAP CRM is transferred to SAP Jam using the notifications mechanism of SAP NetWeaver Gateway if an SAP CRM business object is changed.

Social collaboration application users have access to this information as a result of their access to the related SAP Jam group or some of the Feed Updates that they receive.

If you are using the add-on CRMSWI01 there are several additional authorization aspects you have to consider regarding business object change notifications:

- If a user wants to subscribe to receive change notifications for a specific CRM business object, the display authorization for this business object is explicitly checked.

  Furthermore, the user must be allowed to create subscriptions.

  This is checked by a business object type-dependent BAdI implementation of BAdI /CRMSWI01/SWIGW_SUBAUTH_BADI method CHECK_SUBSCRIBE_AUTH.
- If a notification is created for a subscriber by SAP NetWeaver Gateway, the application is not executed with the privileges of the subscribing user but with the privileges of the end user who changed the business object. Therefore, there is no authorization check based on the subscriber privileges to ensure that the subscribing user still has the same authorizations that were present at the time of subscription.

  For more information, see SAP NetWeaver Gateway Security Guide.

  This means that if a notification is created for a specific CRM business object, it is possible that the subscribers privileges have changed meaning that the subscriber should no longer be able to see this specific business object.

  To enable you to minimize such situations, several checks have been introduced within the add-on.CRMSWI01.

  These checks are performed by a business object type-dependent default BAdI implementation of BAdI /CRMSWI01/SWIGW_SUBAUTH_BADI method CHECK_RECEIVER_AUTH:
  - Check display authorization measured using the business object repository (BOR) framework
  - Check display authorization via ACE for the current business object
  - Check for authorization changes with regard to:
    - Changes of organizational assignment
    - Changes of territory assignment
    - Changes of user role assignment

    You have to schedule the periodic execution of the following report: Package: /CRMSWI01/SWIGW_NOTIFICATION, Name: /CRMSWI01/SWIGW_NTF_CHECK.

    This report performs the checks mentioned above for a given list of business object types. If a change is detected for a specific business object type, the user will be blocked from receiving notifications for the business objects of that type.

    The authorization changes detected by the report are stored in DB table /CRMSWI01/CRMD_SWIGB.

    The notifications that have been blocked are stored in DB table /CRMSWI01/CRMD_SWIGH.

    The next time a CRM user with blocked notifications logs on to the system and the feeds UI block is displayed, the system rechecks the blocked notifications:

The system rechecks the display authorization of the changed business object again for each blocked change notification for this user: If the user is authorized to see the business object, the system sends the blocked change notifications. If the user is not authorized to see the business object, the blocked notifications are deleted from the database table.

4 Component-Specific Guidelines: Interaction Center

Related Security Guides

Table 266

Application	Guide
SAP NetWeaver Application Server (SAP NetWeaver AS)	*SAP NetWeaver Security Guide*
Business Communication Broker (BCB)	*SAP NetWeaver Security Guide*
Software agent framework	*Security Guide for SAP Customer Relationship Management*
Interaction center manager (IC manager)	*Security Guide for SAP Customer Relationship Management*

Why Is Security Necessary?

Security is necessary because:

- The Interaction Center WebClient (IC WebClient) synchronizes contact attached data from the communication management software. Such data could include personal data or restricted business data such as contract order data and must be protected.
- Interaction center agents (IC agents) can log on to SAP Customer Relationship Management (SAP CRM) and access SAP CRM data such as customer contract data and customer master data. Such customer-sensitive data must be protected.

Technical System Landscape

The following figure illustrates the system landscape:

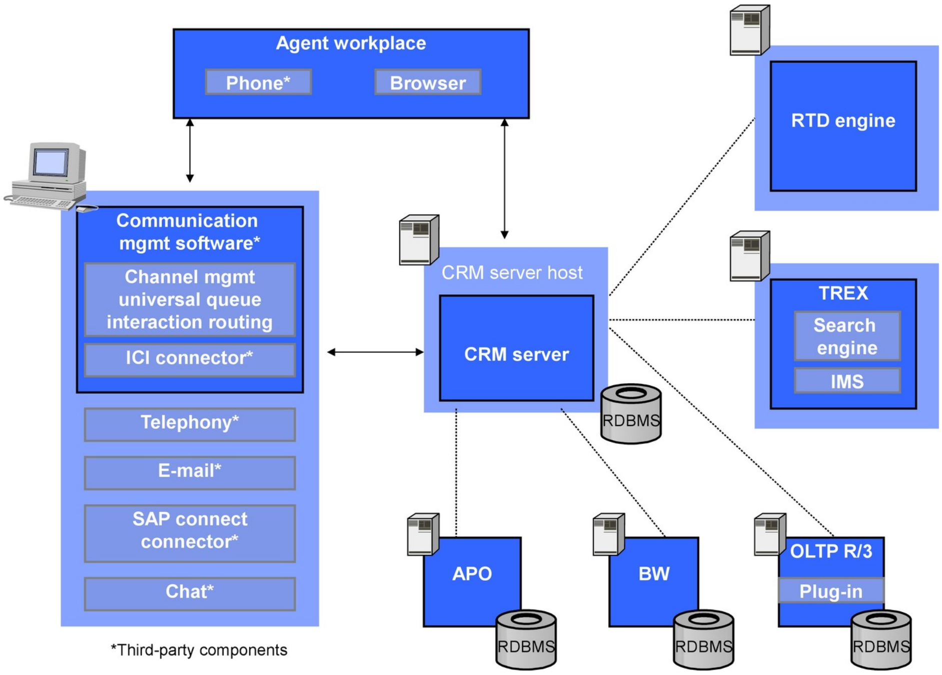


Figure 20: Technical System Landscape

Abbreviation Key for Figure Above

Table 267

Abbreviation	Description
ICI	Integrated Communication Interface
OLTP	Online transaction processing system
RDBMS	Relational database management system
RTD engine	Real-time decisioning engine
SAP APO	SAP Advanced Planning & Optimization
SAP NetWeaver BW	SAP NetWeaver Business Warehouse

Security Aspects of Data Flow and Processes

The figure below shows an overview of the communication channel integration into the IC WebClient:

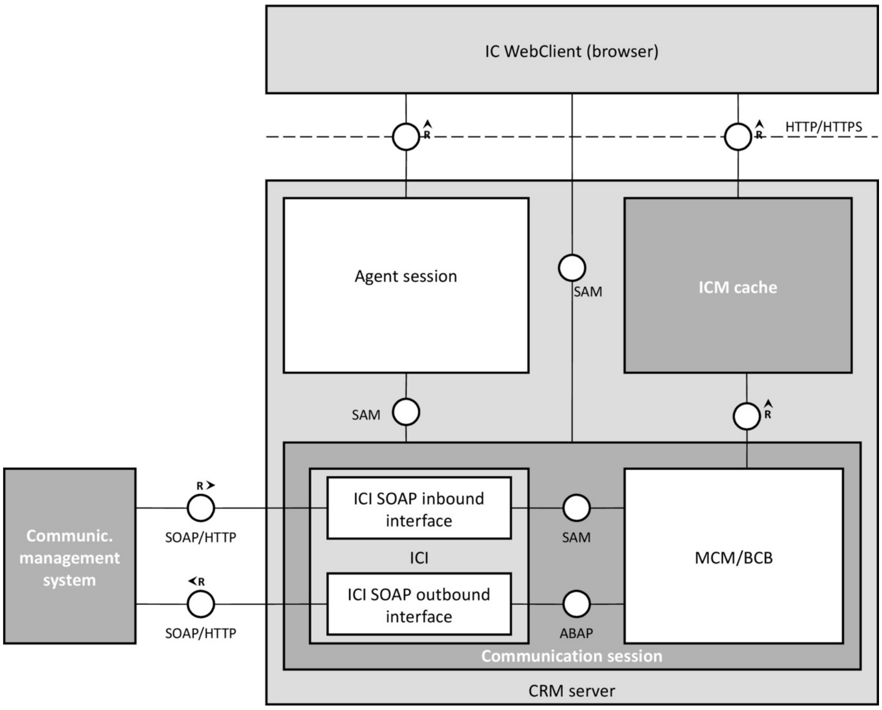


Figure 21: Overview of Communication Channel Integration

The HTTP security session management ensures the security of the communication paths displayed in the graphic. For an overview of the communication paths and more detailed information, see *Communication Channel Security* under *Component-Specific Guidelines: Interaction Center* > *Network and Communication Security*.

Abbreviation Key for Figure Above

Table 268

Abbreviation	Description
ICI	Integrated Communication Interface
ICM	Internet Communication Manager
BCB	Business Communication Broker
MCM	Multi Channel Management
SAM	Simplified ABAP Messaging
SOAP	Simple Object Access Protocol

User Administration and Authentication

The IC WebClient uses the user management and authentication mechanisms provided by SAP NetWeaver, in particular the SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 the Interaction Center. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS ABAP* > *SAP NetWeaver Application Server ABAP Security Guide*.

User Management

Table 269

Tool	Description
User Maintenance (`SU01`) transaction	For more information, see User Administration and Authentication [page 18].
Profile generator (`PFCG`) transaction	You use the profile generator to create roles and assign authorizations to users in ABAP-based systems.

No users are delivered in the standard system. You need to create the following users:

- Remote function call (RFC) user to connect to a back-end SAP ERP system

  This user is optional. You can create it to execute functions in the SAP ERP system from the transaction launcher if you do not want to use the current logon user to connect to a back-end SAP ERP system. The advantage is that, because this user is for RFC use only, it has no system dialog access. Therefore, individuals cannot access the system and cause damage.

  If this user is used, be sure to provide appropriate authorization at the right level (not too much or too little).

- Individual users

  Users on CRM server who can access all capabilities in IC WebClient scenarios

Standard tools are employed for user administration.

Users

Table 270

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user created in *User Maintenance* (`SU01`) transaction	No	Created by an SAP CRM system administrator for accessing the IC WebClient
SAP CRM	Customizing user	No	Dialog user created in *User Maintenance* (`SU01`) transaction	No	Created by an SAP CRM system administrator for customizing the IC WebClient
Back-End SAP ERP	End user	No	Dialog user created in *User Maintenance* (`SU01`) transaction	No	(Optional) Created by an SAP ERP system administrator. This user allows you to use the transaction launcher to access functions from SAP ERP. (User for launch transaction generation depends on the RFC destination – either a specific user or an RFC user.)

System	User	Delivered?	Type	Default Password	Description
SAP ERP	End user	No	Dialog user created in *User Maintenance* (transaction `SU01`)	No	(Optional) Created by an SAP ERP system administrator. This user is for accessing SAP ERP data through employee interaction center.

➡ Recommendation

Users created with a default password must change their password before first use.

User Data Synchronization

If the employee interaction center (EIC)/shared service framework is used, employee data from SAP ERP is replicated to business partner data in SAP CRM and the other way around.

If predictive dialing is used, call list data is synchronized between the SAP CRM system and third-party communication management software (CMS) by the IC manager.

Authorizations

The IC WebClient uses the SAP CRM standard for authorizations.

ABAP Stack Standard Roles Used by SAP CRM

Table 271

Role	Description
`SAP_CRM_UIU_IC_AGENT`	PFCG Role for Interaction Center Agent
`SAP_CRM_UIU_AIC_AGENT`	PFCG Role for Accounting Interaction Center Agent
`SAP_CRM_UIU_IC_AGENT_SSC`	PFCG Role for Interaction Center Shared Service Agent
`SAP_CRM_UIU_IC_ITSDAGENT`	PFCG Role for IC IT Service Desk Agent
`SAP_CRM_UIU_LOY_IC_AGENT`	PFCG Role for Interaction Center Agent for Loyalty Management
`SAP_CRM_UIU_IC_AGENT_EIC`	PFCG Role for Employee Service Center Agent

ABAP Stack Standard Roles Delivered with SAP CRM and Used by Industry Solutions

Table 272

Role	Description
`SAP_CRM_UIU_AUTO_IC_AGENT`	PFCG Role for Automotive Interaction Center Agent
`SAP_CRM_UIU_FCC_AGENT`	PFCG Role for Financial Interaction Center Agent
`SAP_CRM_UIU_FCC_PC_ERP_AGENT`	PFCG Role for Financial Interaction Center Agent – Provider Contract in ERP
`SAP_CRM_UIU_MEDIA_IC_AGENT`	PFCG Role for Media Interaction Center Agent
`SAP_CRM_UIU_PROVIDER_IC_AGENT`	PFCG Role for Telco Provider Interaction Center Agent

Role	Description
SAP_CRM_UIU_TELCO_FCC_AGENT	PFCG Role for Telco FCC Interaction Center Agent
SAP_CRM_UIU_UTIL_IC_AGENT	PFCG Role for Utilities Interaction Center Agent
SAP_CRM_UIU_UTIL_IC_LEAN_AGENT	PFCG Role for Utilities Interaction Center Agent
SAP_CRM_UIU_RETAIL_IC_AGENT	PFCG Role for Retail Interaction Center Agent

If the SAP NetWeaver Portal is used to access IC functions, make sure that you match roles between the SAP NetWeaver Portal and the SAP CRM server.

Standard Authorization Objects

Authorization objects for the different business objects that are used, such as business partners or business transactions, are used in the IC agent scenario. These authorization objects are listed in the respective PFCG roles. For more information about these authorization objects, see the respective sections of the SAP CRM security guide.

The following table shows the security-relevant authorization objects used in the IC agent scenario:

Table 273

Authorization Object	Field	Value	Description
CRM_CATEGO	ACTVT (Activity) SC_ID (Application ID) LN_TYPE (Object links) SC_PART (Part) ASP_STATE (Schema status)	N/A	(Optional) This authorization object is used in the auto suggest function in the IC WebClient. For more information, see SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Basic Functions* › *Multilevel Categorization* › *Authorizations for the Category Modeler* .
S_RFC	ACTVT RFC_NAME RFC_TYPE	16 CRM_ICI_HBT FUGR	(Optional) This authorization is needed for a remote function call (RFC) used by the heartbeat function, which is activated through functional profile ICI_HEART_BEAT.
SMI_AUTH	SMI_ACTVT (Processing Type)	*Display*, *Create*, *Change*, *Delete*	This authorization object controls access to social media posts and social media user data.

The following authorizations are only relevant for the shared service framework scenario:

Table 274

Authorization Object	Field	Value	Description
S_RFC	ACTVT RFC_NAME RFC_TYPE	16 CRM_IC_SSC_COLL FUGR	Used for miscellaneous inbound RFCs to trigger business functions from an external system
S_RFC	ACTVT	16 CRM_IC_AUI_ASYN	(Optional) This authorization is needed for an RFC used by

Authorization Object	Field	Value	Description
	`RFC_NAME` `RFC_TYPE`	`FUGR`	the asynchronous inbox search.

Note

In a shared service scenario, the corresponding users in the external systems (such as SAP ERP) need the necessary authorization to execute the business functions that are triggered (by RFCs or launch transactions). For more information about which authorizations are necessary, see the security guides and documentation for those systems.

Authorizations for Accelerated Agent Inbox Search

The following information is relevant if SAP HANA is your primary or secondary database:

If you are using the accelerated agent inbox (inbox) search, you must set up authorizations in the SAP HANA system. For more information, see SAP Help Portal at help.sap.com/crm > *<Choose relevant release>* > *Application Help* > *Interaction Center* > *Interaction Center WebClient* > *Agent Inbox in the Interaction Center WebClient* > *Accelerated Inbox Search* > *Setting Up the Accelerated Inbox Search*.

Network and Communication Security

Communication Channel Security

Table 275

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Communication between a Web browser and SAP NetWeaver AS	HTTP/HTTPS	User requests are transferred between a Web browser and SAP NetWeaver AS. Logon information and subsequent requests from the browser are transferred from the browser to SAP NetWeaver AS.	Used when IC agents log on to CRM server from a Web browser. User-sensitive data must be protected. To configure secure sockets layer (SSL) over SAP NetWeaver AS, see *SAP NetWeaver Security Guide*.
Communication channel between components residing in different ABAP sessions of IC WebClient	HTTP/HTTPS	Each IC WebClient application session consists of multiple ABAP sessions running concurrently.	Used when IC WebClient is initiated. To enable HTTPS, an additional HTTP destination is created (see the *Communication Destinations* section below). To configure SSL over SAP NetWeaver AS, see *SAP NetWeaver Security Guide*.
Communication between a remote SAP CRM system or a remote SAP ERP system	HTTP through SAP Internet transaction server (SAP ITS); SAP ITS connects to the remote SAP CRM system or	Business transactions and business objects are exchanged between SAP ERP and SAP CRM.	(Optional) Used when an IC agent in SAP CRM tries to access data in an SAP ERP system or a remote SAP CRM

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
	SAP ERP system through RFC		system by launching a transaction. Used when creating and prepopulating a service request from a remote SAP ERP system.
Communication within the same SAP CRM system	HTTP through UI	N/A	(Optional) Used when an IC agent tries to launch a UI application on the same CRM server by launching a transaction. Configure HTTP over SSL in SAP NetWeaver AS.
Communication between a SAP CRM system and communication management software (CMS), such as telephony or e-mail routers	Business communication broker (BCB) application programming interface (API) communicates with the CMS using the Simple Object Access Protocol (SOAP)	Data (such as incoming call, contact attached data, and e-mail) is transferred from the CMS to the SAP CRM system.	(Optional) Used when multichannel is used in the IC WebClient to handle telephone calls, e-mails, chat, and so on.
Communication between an SAP CRM system and a third-party telephony switch	SAPphone API communicates with the third-party telephony switch using RFC	Incoming call data is exchanged.	(Optional) Used when IC agents handle telephone calls through SAPphone.
Communication between SAP CRM and TREX	SOAP through TREX API	N/A	(Optional) Used when IC agents require the knowledge search through the TREX search engine. For more information, see SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Interaction Center* › *Interaction Center WebClient* › *Knowledge Search in SAP CRM*.
Communication between SAP CRM and the real-time decisioning engine (RTD engine)	SOAP over HTTP/HTTPS	Events on user actions are sent to the RTD engine. Offers are received through the RTD engine.	(Optional) Used when the RTD engine is integrated into IC for real-time offer management
Communication between SAP CRM and Solution Manager	RFC and WebService	Incidents (both directions), IBase from Solution Manager to SAP CRM	Optional

Network Security

The Business Server Page (BSP) ports for HTTP/HTTPS have to be opened in the firewall if one or both of the following are true:

- There is a firewall between agents' machines and the CRM server
- Agents access the IC WebClient from another network or from the Internet by launching the IC BSP URL

Communication Destinations

The table below shows an overview of the communication destinations used by the IC WebClient:

Table 276

Destination	Delivered?	Type	User, Authorizations	Description
TREX server	No	HTTP	N/A	(Optional) Part of the TREX configuration
Remote SAP CRM system	No	RFC	N/A	(Optional) Communication to a remote SAP ERP system or a remote SAP CRM system through the transaction launcher
SAP ERP	No	RFC	N/A	(Optional) Communication to a remote SAP ERP system through the transaction launcher. This is out of scope of IC WebClient. It is part of the Business Object Repository (BOR) setup.
SAP ERP	No	RFC	N/A	(Optional) Communication to SAP ERP to retrieve employee data if you are using the employee interaction center (EIC).
SAP Solution Manager	No	RFC WebService	N/A	(Optional) Communication to a remote SAP Solution Manager system
Third-party telephony server	No	RFC	N/A	(Optional) Only if IC agents handle calls using SAPphone.
RTD engine	No	HTTP/HTTPS	N/A	(Optional) Only if real-time offer management is activated in the IC WebClient.

You must add the following additional communication destination for HTTPS:

Table 277

Destination	Delivered?	Type	User, Authorizations	Description
Connection between two different IC sessions	No	RFC	SSL is activated	Created by a system administrator using the `CRMM_IC_GFS` transaction to set up the communication between different IC WebClient sessions (agent session, worker session, or SAPphone session).

Internet Communication Framework Security

You should only activate the services that are needed for the applications running in your system.

In case of an integration with the real-time decisioning engine (RTD engine) in the IC WebClient, you have to use service CRM_IC_RE_WS. You can activate this service in transaction SICF.

If your firewall(s) use URL filtering, also take note of the URLs used for the services and adjust your firewall settings accordingly.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Activating and Deactivating ICF Services*.

For more information about ICF security, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for Connectivity and Interoperability Technologies* › *RFC/ICF Security Guide*.

Data Storage Security

Stored Data

Table 278

Data	Stored Where	Stored When	Type of Access
Customizing	SAP NetWeaver AS database	After installation	Read/write/change/delete Only by user with SAP CRM Customizing authorization
Application data	SAP NetWeaver AS database	IC user logon/request	Read/write/change/delete
Generated class	SAP system	During Customizing of transaction launcher	Read/write/change/delete
Configuration	SAP system	After installation	Read/write/change

The IC WebClient requires a Web browser as the user interface. The data is stored on the CRM server.

All data stored in the SAP CRM system is protected by the SAP CRM back end. Customizing data can be accessed only by persons with SAP CRM Customizing authorization. This data is accessed by the system administrator during system configuration. Application data is protected by the authorization object. Roles define the authorization. Users assigned to a role inherit authorization from the role.

The simplified ABAP messaging (SAM) component stores HTTP(S) URLs of the different ABAP sessions of the IC WebClient as server-side cookies. (Each IC WebClient application session consists of multiple ABAP sessions running concurrently.) This URL contains the session ID of the ABAP session. This data is not sensitive and is not accessible from outside the current application server (AS), so there is no severe security risk. This information is deleted from the server-side cookie once the application session is shut down.

Security for Social Media Integration in Interaction Center

- You can use the authorization object `SMI_AUTH` to control authorization for social media posts and social media user data. You can control authorization for displaying, creating, changing, and deleting data.
- If you are retrieving social media posts with attachments, you must carry out a virus scan to ensure the security of the attachments. For more information about virus scans, see the*Virus Scan Profiles* subsection of the Network and Communication Security [page 29] section.

Security for Text Message Integration in Interaction Center

- If you are configuring SAPconnect for sending text messages, check the security-related settings. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform ›

<Choose relevant release> › *Application Help* › *Function-Oriented View* ›: Search for *SAPconnect (BC-SRV-COM)*.

- For general security information regarding RFC scenarios, see SAP Library for SAP NetWeaver on SAP Help Portal at › help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for Connectivity and Interoperability Technologies* › *RFC/ICF Security Guide* ›.
- If the default connector, which uses SAPconnect, does not meet your requirements in terms of the dedicated service provider, you can use a customer-defined connector. In this case ensure that the network communication is secure. For more information see the Network and Communication Security [page 29] section.
- Authorization concept for text message integration in interaction center:
  - Triggering text messages: The text message is triggered by sales order actions. If a business user has the authorization to change the sales order, there will be no additional authorization checks for the text message.
  - Displaying text messages: The entry of the outbound plug mapping `CRM_SMS` is enhanced for text messages in the navigation bar profile `IC_AGENT` or `IC_SSC_AGENT`. The entry is assigned to the `PFCG` roles `SAP_CRM_UIU_IC_AGENT` and `SAP_CRM_UIU_IC_AGENT_SSC` to control the authorization for displaying text messages.

Security for Additional Applications

The following additional applications are associated with the IC WebClient or delivered with it:

- Third-party communication management software (CMS)

  This has its own authentication and authorization mechanism to ensure security. Presently it does not support HTTPS communication.
- Business communication broker (BCB)
- SAPphone

  Provides a telephony function for the interaction center (IC).
- SAP Customer Activity Repository

  This is a separately licensed application for IS-Retail that you integrate with SAP CRM and SAP ERP for multichannel scenarios. SAP Customer Activity Repository contains the multichannel sales repository, into which SAP CRM replicates business partner data, and SAP ERP replicates sales order information.

There are no particular front-end clients that deviate from the standard SAP system.

The following table lists details for the additional applications

Table 279

Additional Application	Vendor	Security Guide	Special Security Settings
SAP ITS	SAP internal	*SAP NetWeaver Security Guide*	No
UI	SAP internal	*Security Guide for SAP Customer Relationship Management*	To use the UI-based application within the IC WebClient, users must have authorization to start the UI-based application
BCB	SAP internal	*SAP NetWeaver Security Guide*	No

Additional Application	Vendor	Security Guide	Special Security Settings
SAPphone	SAP internal	N/A	No
SAP Customer Activity Repository	SAP internal	*SAP Customer Activity Repository Security Guide*	No

Other Security-Relevant Information

Table 280

Active Code	Location	Functions Disabled Without This Active Code
Java applet	Free seating	Free seating is an IC capability that allows agents to utilize communication services provided at different workplaces.
JavaScript	Widely used in front end	IC WebClient

One Java applet is used in the IC agent application. We recommend running this applet in the intranet because it is not digitally signed.

All users must ensure that the scripting Java applet is enabled in their Internet browser.

Trace and Log Files

The following information is traced in the AS cache:

- Messages exchanged between CMS and the CRM server
- Messages exchanged between ABAP sessions

Trace is turned off by default. To turn on the trace and change the trace level, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Administration of the Internet Communication Manager*.

For integration of the RTD engine, a separate trace can be turned on. This traces all messages exchanged between the RTD engine and the CRM server. This trace is turned off by default.

4.1 E-Mail Response Management System

The E-Mail Response Management System (ERMS) is based on SAP NetWeaver Application Server (SAP NetWeaver AS) and SAP Customer Relationship Management (SAP CRM). ERMS runtime runs on top of the workflow system. The design time uses the UI framework.

Related Security Guides

Table 281

Application	Guide
SAP NetWeaver AS	*SAP NetWeaver Security Guide*
Workflow	*SAP NetWeaver Security Guide*

Why Is Security Necessary?

The ERMS deals primarily with e-mail. The openness of this communication channel allows anyone to send an e-mail to this system. The following measure ensures the following:

- High availability of the system (that is, make sure the system is not brought down by massive numbers of requests)
- Protect the system from e-mails containing malicious content
- Protect data that is important in this application (such as personal information within the SAP CRM system)

Technical System Landscape

The following figure illustrates the technical system landscape:

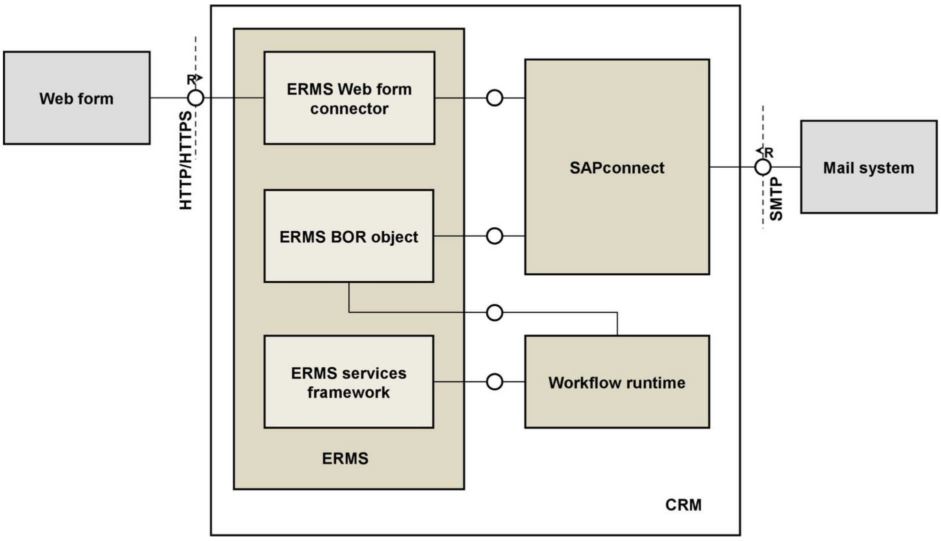


Figure 22: Technical System Landscape

The entry point to ERMS runtime is SAPconnect. Once an e-mail is received by SAPconnect, it hands over the e-mail item to ERMS BOR object `ERMSSUPRT2`. This starts the execution of workflow `ERMS1`. You can associate an e-mail address in the system with this ERMS BOR object in the *Inbound Distribution: Settings for Recipient Determination* (`SO28`) transaction. Once the workflow is triggered by the incoming e-mail, it starts the ERMS service manager.

User Administration and Authentication

User Management

For general information about user management in SAP CRM, see the User Management [page 18] section.

User Management Tools

Table 282

Tool	Description
User Maintenance (`SU01`) transaction	N/A
Profile generator (`PFCG`) transaction	You use the profile generator to create roles and assign authorizations to users in ABAP-based systems.

No users are delivered. You need to create the following users:

- Background user

  User for executing workflow tasks in the background
- Individual users

  In addition to creating the above workflow user above, it is necessary to do the following:

- ○ Give the system administrator access to modeling tools available for the ERMS
- ○ Create users for interaction center agents (IC agents) so that they can access the system and process incoming e-mails

Users

Table 283

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog	No	Created by an SAP CRM system administrator for access to the IC WebClient
SAP CRM	Background user	No	System	No	For executing workflow tasks in the background
SAP NetWeaver Business Warehouse (SAP NetWeaver BW)	ERMS administrator or IC manager	No	Dialog	No	For access to ERMS reports in SAP NetWeaver BW

> ➡ Recommendation
>
> Users created with a default password must change the password before first use.

User Data Synchronization

Reporting data is stored initially in SAP CRM. For historic reporting, it must be transferred to the SAP NetWeaver BW system.

Authorizations

The ERMS uses the SAP CRM standard for authorizations.

To enable ERMS administrators to use the ERMS design-time tools (such as the profile generator), you must assign ERMS administrators to the SAP CRM role `SAP_CRM_UIU_IC_MANAGER`. This role includes the necessary authorization to access the following tools:

- Rule modeler
- Category modeler
- ERMS reporting
- E-mail workbench

In addition, authorization groups make it possible to restrict different permissions (read, write, deploy, and so on) in the rule modeler. You can maintain authorization groups in Customizing for *Customer Relationship Management* under ▶ *E-Mail Response Management System* ▶ *Define Repository* ◀. Select the appropriate context (such as *ERMS*) and select *Authorization Groups*.

Finally, add authorization `CRM_ERMS_P` to role `SAP_CRM_UIU_IC_MANAGER`, and set the following parameters accordingly:

- Activity
- ERMS authorization group
- Context

Network and Communication Security

Communication Channel Security: E-Mail

We recommend that you use a general purpose e-mail server, such as Microsoft Exchange. You must implement a virus scanner on the e-mail server to scan e-mails or e-mail attachments. After scanning, the e-mail is handed over to the ERMS for processing. If you allow HTML e-mails, you must install a filter for script on your e-mail server.

SAPconnect uses Simple Mail Transfer Protocol (SMTP) for receiving e-mails. Another option for configuring your system is to send an e-mail directly to the SAP CRM system and have it processed by the ERMS. Note that this latter option is not recommended. For more information about SAPconnect, see SAP Note 738326.

To display or process HTML content of e-mails within the interaction center, your e-mail infrastructure must be able to secure or sanitize HTML mails with active content (such as, but not limited to, JavaScript) before they are sent to the interaction center. You must also guarantee that measures for securing or sanitizing these mails (for example filtering on the e-mail server) are switched on.

If you cannot guarantee that such measures are in place, you can disable or filter the display of HTML e-mails in the interaction center as follows:

1. Configure the display of HTML e-mails.

   You do this in Customizing for *Customer Relationship Management* under ▶ *Interaction Center WebClient* › *Basic Functions* › *Communication Channels* › *Define E-Mail Profiles* ◀, by setting the field *Disp. HTML Mail* (Display of HTML Mails) to *Disabled* or *Filtered*.

   If you filter the display of HTML e-mails, the system triggers a warning message if a user opens an HTML e-mail that contains non-secure content. The user can decide whether the e-mail sender is trustworthy before displaying the entire content of the e-mail.

2. Assign the corresponding e-mail profile to each business role that uses the e-mail editor in the agent inbox (standard role IC Agent) or the ERMS e-mail workbench (standard role IC Manager).

   In Customizing for *Customer Relationship Management*, choose ▶ *Interaction Center WebClient* › *Define Business Role* ◀, and choose the step *Assign Function Profiles*. The relevant function profile ID for e-mail profiles is `EMAIL`. The value assigned to the function profile `EMAIL` should be the e-mail profile ID that you have changed in the first step. If there is no entry for the function profile `EMAIL`, you have to add one.

You can also define an ERMS rule to handle, that is delete, incoming HTML mails and inform the sender automatically that you are not able to view HTML mails. HTML mails can be recognized by the e-mail document type HTM in the ERMS rule modeler after adding the following Customizing: In Customizing for *Customer Relationship Management*, choose ▶ *E-Mail Response Management System* › *Define Repository* ◀. Choose the context *ERMS* and go to the step *Attributes*. Add the following entry:

Attribute: <Attribute ID> (for example, ZMAIL_DOCTYPE)

Description: E-Mail Document Type

Show Attribute: X

XPath: /paths/EMAIL/OBJ_TYPE/text ()

Fact Gathering Service: FG_EMAIL

Attribute Extension Class: CL_CRM_ERMS_ATTR_EXT_EQUALS

Communication Channel Security: Specifics for E-Mails Received Through the Integrated Communication Interface

You can use the virus scan profile */IC_CCS_MCM/ICI_MAIL* to enable the scanning of e-mails that enter the system through the Integrated Communication Interface. If the connected virus scanner detects malicious content within the e-mail or the attachment after the activation of the profile, the e-mail and the attachment respectively are replaced by an error message. The same applies if the e-mail or attachment does not comply with MIME type restrictions set up in the profile.

For more information, see Customizing for Customer Relationship Management under *Interaction Center WebClient* > *Basic Functions* > *Communication Channels* > *Define Virus Scan Profiles for ICI Mail*.

Communication Channel Security: Web Form Connector

If you are using the web form connector, you must do the following to handle undefined web form IDs:

- Create a default implementation of BAdI `CRM_ERMS_WF_CON`.

  In the BAdI implementation, form data from undefined web form IDs must be rejected.
- Submit the form data to the `confirmation.htm` BSP page.
- Ensure that the form data has successfully passed a `CAPTCHA` before it is submitted to the web form connector.

Data Storage Security

ERMS data is stored in the CRM database like any other SAP CRM information. It is not necessary to add security. The stored data can be classified as shown in the following table:

Stored Data

Table 284

Data	Stored Where	Stored When	Type of Access	Who Can Access It
E-mail document	SAP CRM system under business workplace persistence Database table `CRMD_ERMS_CONTNT`	When an e-mail arrives	Read/delete	ERMS routes the e-mail to an organizational unit. Users in that organization can access the e-mail document.
ERMS fact base	SAP CRM system under workflow container	When ERMS processes an e-mail	Read/write/delete/change	IC manager in the ERMS log, or the *Selection Report for Work Items* (`SWI1`) transaction (only in read-only mode)
ERMS rules	Customizing for *Customer Relationship Management* under *E-Mail Response Management System* > *Define Repository*	When rules are maintained	Read/write/delete/change	IC manager
ERMS configuration	SAP CRM system under ERMS repository (Customizing data)	During configuration	Read/write/delete/change	ERMS administrator Person who makes the Customizing settings for *Customer Relationship Management*
ERMS reporting data	SAP CRM system under ERMS reporting data	At different points during e-mail processing (manual and automatic) and	Read/write/delete/change	ERMS administrator IC manager

Data	Stored Where	Stored When	Type of Access	Who Can Access It
		when ERMS reporting data is maintained		

Trace and Log Files

Log information is available in *Check Automatic Processing Details* (transaction `CRM_ERMS_LOGGING`). The log provides the following information:

- Services by ERMS service manager
- Data gathered by ERMS services
- Rules evaluated
- Categories assigned
- Execution times for different services

Checklist

Table 285

Feature	Check	How to Check
Restrict access to e-mail processing	Workflow e-mail task can be processed only by authorized organizational units or authorized users	On the SAP Easy Access screen, choose ▶ *Interaction Center* › *E-Mail Response Management System* › *Settings* › *Assign Agent for E-Mail Handling* ◀. Choose *Assign Agents*. Expand workflow template *ERMS1* and select task *TS 00207914*. Choose *Attributes* and select the item as required. In the toolbar, choose *Create agent assignment*. (Not necessary for a general task because everybody can process this task.)
Restrict access to e-mail processing	Authorized agents are properly assigned to the organizational unit	For the e-mail workflow task above, on the SAP Easy Access screen, choose ▶ *Interaction Center* › *Supporting Processes* › *IC Structure* › *Change Organization and Staffing* ◀.
Restrict or allow access to certain policies in ERMS rule modeler	ERMS authorization group concept is used	To define your authorization groups, use transaction `CRMC_ERMS_REPOSITORY`. To define which policies users can read, change, create, and deploy, and under which ERMS authorization groups such operations can be performed, use authorization object `CRM_ERMS_P` as a template.

Feature	Check	How to Check
Web form connector (if used)	Default implementation for the *ERMS Web Form Connector BAdI* (CRM_ERMS_WF_CON) exists	1. In the *BAdI Builder* transaction (SE18), display the BAdI CRM_ERMS_WF_CON. 2. Ensure that the *Enhancement Implementations* tab page contains a BAdI implementation in which the *Default Implementation* checkbox is selected.

4.2 Interaction Center Manager

The interaction center manager (IC manager) includes the following components:

- IC manager dashboard (application component CRM-IC-MDB)
- IC analytics, including interaction statistics and interactive scripting (application component CRM-ANA-IC)

Related Security Guides

Table 286

Application	Guide
SAP NetWeaver Application Server (SAP NetWeaver AS)	*SAP NetWeaver Application Server Security Guide*

Why Is Security Necessary?

Security is necessary to prevent attacks from the Internet and to protect data.

The IC manager can access the SAP CRM system using a Web browser, even if the IC manager does not have a user in SAP Customer Relationship Management (SAP CRM). Hence, the authority of the IC manager with regard to system access has to be defined. For example, you should consider whether to allow an IC manager to delete a program after logging on to a back-end SAP CRM system using the browser.

The IC manager can perform functions such as monitoring each agent’s call status, designing scripts to guide the agents, and broadcasting messages to agents. For this reason, care must be taken that the IC manager is assigned only to the desired persons. Otherwise, misleading information could be broadcast to agents, or critical information can be stolen.

User Administration and Authentication

User Management

User management for the IC Manager uses the mechanisms provided with the SAP NetWeaver AS ABAP, for example, tools, user types, and password policies.

User Management Tools

Table 287

Tool	Description
User Maintenance (SU01) transaction	N/A

Tool	Description
Profile generator (PFCG) transaction	You use the profile generator to create roles and assign authorizations to users in ABAP-based systems.

No standard users are delivered.

You need to create an SAP CRM user. If users want to access IC manager functions, we recommend that the system administrator creates users and assigns them to CRM_UIU_IC_MANAGER (for more information, see the *Authorizations* section below). All functions for the IC manager are defined in this role.

Users

Table 288

System	User	Delivered?	Type	Description
SAP CRM	End user	No	Dialog	Created by an SAP CRM system administrator
SAP NetWeaver Business Warehouse (SAP NetWeaver BW)	End user	No	Dialog	Created by an SAP NetWeaver BW system administrator

> Note
>
> The default password for the SAP CRM system and the SAP NetWeaver BWI system is necessary when creating a new user in those systems. When you create new users with an initial password, we recommend that the new users log on to the back-end system to change the initial password.

User Data Synchronization

All data is stored in the SAP CRM system. There is no user data synchronization.

Integration with Single Sign-On Environments

The application accepts SAP logon tickets.

The application does not accept X.509 digital certificates.

Authorizations

The IC manager uses the SAP CRM standard for authorizations.

No roles are delivered with this application. However, one back-end role (SAP_CRM_UIU_IC_MANAGER) is delivered with the SAP CRM back end. This role corresponds to the IC manager role, which is delivered with several versions of the SAP CRM business package.

The following table shows the security-relevant authorization objects used in the interaction center manager (IC manager) scenario:

Standard Authorization Objects

Table 289

Authorization Object	Field	Value	Description
CRM_BM	ACTVT: Activity	16	Only users with this authorization in their user

Authorization Object	Field	Value	Description
			profile can start the broadcast messaging server application for IC manager.
S_RFC	ACTVT RFC_NAME RFC_TYPE	16 CRM_IC_SCRIPTING_PERSIST CRM_IC_XML_STORAGE FUGR	This authorization object is used in the interactive scripting editor to access two function groups: CRM_IC_SCRIPTING_PERSIST CRM_IC_XML_STORAGE
CRM_ERMS_P	ACTVT ERMS_CTXT ERMS_AUGR	01, 02, 03, 43 Any context defined in Customizing (transaction CRMC_ERMS_REPOSITORY) Any authorization group defined in Customizing (transaction CRMC_ERMS_REPOSITORY)	This authorization object defines which rule policies the IC manager is allowed to work with and what activities within them are permitted.
CRM_IC_SCR	ACTVT SCR_GRP	02, 03, or 06	This authorization object is used to protect certain groups of scripts so that only a limited number of managers can access, display, or delete them.
CRM_IC_MDB	ACTVT	16	This authorization object is used when the manager dashboard is started.

Network and Communication Security

Communication Channel Security

The IC manager application runs in the Web browser and it needs to communicate with the back-end CRM server. For this, an HTTP(S) communication channel is required.

- Broadcast messaging
  - HTTP(S) communication from browser to CRM server
  - HTTP(S) communication between CRM servers for sending messages to agents
- IC manager dashboard
  - HTTP(S) communication from browser to CRM server
  - Communication between CRM server and communication management software (CMS) using Simple Object Access Protocol (SOAP)

Data Storage Security

No temporary data is stored. This is a Web-based application.

Broadcast messaging uses cookies to store certain UI favorites on the client side. This data is retained until it is manually deleted. No sensitive data is stored in the cookie, so there are no specific measures to protect the cookie.

The IC manager dashboard stores personalization data (such as application layout) on the client side. This data does not require further security protection.

Other Security-Relevant Information

Refer to the security policy before using active code and the IC manager dashboard.

> ⚠ Caution
>
> Using active code such as applets and ActiveX controls can pose a security risk.

Active Code

Table 290

Application	Active Code	Functions Affected
Interactive scripting editor	Java plug-in	Interactive scripting editor cannot be started

Checklist

Table 291

Feature	Check	How to Check
Broadcast messaging for supervisors	For authorization object `CRM_BM`, check that field `ACTVT` has a value of 16	In the profile generator (`PFCG`) transaction, enter role `SAP_CRM_UIU_IC_MANAGER` or any role used to create supervisors, and choose *Display*. On the *Authorizations* tab, choose *Display Authorization Data*. Choose ▶ *Utilities* › *Technical names on* ◀.
Interactive scripting editor	For authorization object `S_RFC`, check that: Field `ACTVT` has a value of 16 Field `RFC_NAME` has a value of `CRM_IC_SCRIPTING_PERSIST` or `CRM_IC_XML_STORAGE` Field `RFC_TYPE` has a value of `FUGR`	Same as above
Interactive scripting editor	For authorization object `CRM_IC_SCR`, check that: Field `ACTVT` has a value of 02, 03, or 06 Field `SCR_GRP` has a value of [blank]	Same as above

5 Component-Specific Guidelines: Field Applications

Field applications enable you to use the marketing, sales, and service functions in an offline environment for sales representatives and service technicians who work in the field. Field sales representatives and service technicians can access and update customer relationship data on their notebooks while they work in the field.

This section describes security-relevant information for the following field applications:

- SAP Mobile Sales
- SAP Mobile Service

5.1 SAP Mobile Sales

The security information in this topic is relevant for all mobile client applications, such as SAP Mobile Sales and SAP Mobile Service.

Important SAP Notes

Table 292

SAP Note Number	Title
686684	Tile authorizations are the same across the application
628401	Unable to logon Mobile client with Windows normal users
559410	Log on and Password Maintenance Functionality in 4.0
694071	Log on to application fails using Winlogon
622748	Workgroup Login Failure: Creation of Crypting Object Failed
792979	Encrypting the user database password on Mobile clients
1525994	Apache Tomcat on MSA is accessible from network
1617080	Directory Traversal in Mobile Sales BW Workbook

User Administration and Authentication

User Management

You can assign multiple business partners with the role *Employee* to a site (mobile client). For every employee, a user can be created in SAP Customer Relationship Management (SAP CRM) using the administration console.

The standard system contains the following replication functions:

- Employees have *Bulk* replication using the *Employee* publication.
- Users have *Intelligent* replication using the *Users (By Employee)* publication.

For a connected site, all employees are available. However, users are available for only those employees that need to log on to a mobile client application.

During the first logon to a mobile application, the user must change the default password `init` to a unique password. Replication of data from the CRM server is triggered by users using ConnTrans. Once the synchronization is complete, data is imported into the user database, and all business components of the application are updated simultaneously.

User Types

Apart from a demo database, there are no other user types delivered with a mobile application. The customer must create users using the administration console in SAP CRM. According to the defined subscription, only those users that are created for the mobile client's site are replicated to all mobile clients.

The system administrator at the customer's site creates individual interactive users. Only one technical user, which is for the Internet demo and evaluation system (IDES), is delivered with the mobile application.

Table 293

System	User	Delivered?	Type	Default Password	Description
User database (SQL Server)	IDES	Yes	Technical user	IDES ➡ Recommendation We recommend that you change this default password when you log on to the user database.	This user is used to access the user database (SQL server). Data for the technical user is stored in the local registry. The password can be encrypted.

User Data Synchronization

Synchronization of the mobile application with the consolidated database (CDB) of SAP CRM is performed using ConnTrans. Synchronization can be triggered by users any number of times and at any point in time.

For more information, see Mobile Client Synchronization [page 233].

Integration with Single Sign-On Environments

There is no integration with single sign-on (SSO) environments. Mobile applications do not accept any logon tickets or X.509 digital certificates.

Authorizations

You can define authorizations using the mobile authorization management tool (AMT). Certain predefined roles are shipped for an AMT user. For more information about AMT, see SAP Library for SAP Customer Relationship Management on SAP Help Portal at help.sap.com/crm.

> **Note**
>
> Authorization is disabled with the default installation of mobile applications.

Network and Communication Security

For more information, see Mobile Client Synchronization [page 233].

⚠ Caution

For network security reasons, you must implement SAP Note 1525994.

Data Storage Security

Data for mobile applications is stored in the user database (SQL server) on the mobile client. Users can create, change, and delete all types of business objects and business data in a mobile application. All changes are immediately updated in the user database. In addition to this, certain temporary files are stored in the local file system of the mobile client under `WindowsUser\%Temp%`.

Using Logical Path and File Names to Protect Access to the File System

In the process of providing mobile clients with workbook data from SAP BW, temporary data is saved in files in the file system on the SAP CRM application server. In order to prevent that existing files are overwritten, it is important to adhere to a naming convention as well as directory structure. This is achieved by specifying logical paths and file names that map to the physical paths and file names. This mapping is validated at runtime in order to generate files within the correct name range. The following lists show the logical file names and paths used in this context and for which programs these file names and paths apply.

Logical File Names Used in the Context of Transaction Manage and Monitor BW Requests for Mobile Clients (SMOBILEBW)

The following logical file names have been created in order to enable the validation of physical file names:

- Logical file name `SMO2_BWA`:
  - Programs using this logical file name:
    - `SMO2REQMAINTAIN`
    - `SMOBWREQ`
    - `SMOBWREQ2`
    - `LSMO2_REQUESTF01`
    - `LSMO2_REQUESTU06`
    - `LSMO2_REQUESTU28`
  - In this context, parameter `<PARAM_1>` *Report ID* is used.

    We recommend to define the physical file name as `BWA_<PARAM_1>`.
- Logical file name `SMO2_MEMO`:
  - Programs using this logical file name:
    - `SMO2REQMAINTAIN`
    - `SMOBWREQ`
    - `SMOBWREQ2`
    - `LSMO2_REQUESTU30`
  - In this context, parameter `<PARAM_1>` *Request ID* is used.

    We recommend to define the physical file name as `MEMO_<PARAM_1>`

Logical Path Used in the Context of Transaction Manage and Monitor BW Requests for Mobile Clients (SMOBILEBW)

The logical file names listed above all use the logical file path `SMO2_BWA`.

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physcial path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log. For more information, see the following references:

- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Logical File Names*.
- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for the Application Server* › *Security Guides for the AS ABAP* › *SAP NetWeaver Application Server ABAP Security Guide* › *Special Topics* › *Protecting Access to the File System Using Logical Path and File Names*
- SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Security Audit Log*.

Data Protection

Data protection on the mobile client is achieved using subscriptions provided by middleware in SAP CRM. This mechanism allows a system administrator to control what data a specific user can download to a mobile client. This prevents users from accessing or changing data that is not relevant to the user profile.

Example

You create a site of type mobile clients, A001, using the administration console. A user is associated with this site. This user must only receive business partner information based on the postal area code.

To do this, you must first create a publication for *Postal code area customer*, and then define a subscription for this publication. Various sites can now subscribe to this publication. The user can only work on the data that is relevant to the defined user profile

For more information, see the following:

- SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Data Exchange and Mobile Technologies* › *CRM Integration Services*
- *Hard Drive Encryption* subsection below

Minimal Installation

Implement the landscape that is recommended by SAP.

For more information, see the *CRM Mobile Client Installation Guide* on SAP Service Marketplace at service.sap.com/instguides.

All the mobile client components that must be installed are described in the installation guide. These system resources are mandatory for the mobile client components to function properly.

The main difference between a demo and a nondemo system is the database installation. Depending on the selection, either the demo or the nondemo database is installed. Since only the necessary components are installed, you do not have to remove any components from the productive system.

Recommendation

Customers can decide whether the authorization management tool (AMT) is required. We recommend that you use the AMT to restrict certain functions to certain groups of users.

For more information, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *Data Exchange and Mobile Technologies* > *CRM Mobile Technology* > *Authorization Management Tool (AMT)*.

Checklist

Table 294

Feature	Check	How to Check
Set authorizations for the user interface and business object levels of mobile client applications	Is AMT installed?	*Start* > *Programs* > *SAP* > *Mobile* > *AMT*.
	Is AMT activated?	1. Start AMT. 2. Navigate to the *System Maintenance* tile. 3. Select the *Value* checkbox.
Protection of mobile client data if the mobile client (laptop) is stolen	Is the hard drive encrypted?	For more information, see the *Hard Drive Encryption* section below.

Hard Drive Encryption

By stealing hard drives, criminals may attempt to access internal company data, which they can use to cause loss or damage to a company or gain a competitive advantage. To combat the threat of unauthorized access to information, data on local hard drives is encrypted. If, as a user, you want to view your plain text data on the hard drive, you must first enter a password to decrypt such data. Any person attempting unauthorized access without this password can see only indecipherable binary data.

While implementing encryption, the following aspects must be considered:

- Manageability

  When using encryption, you must always ensure good administration of the encryption keys used. Depending on the product, this implies additional planning, management, and administration.
- Encryption technology
- Usability
- Loss of performance

  When accessed, the encrypted data is first decrypted and then encrypted again when it is changed. The loss in performance depends on the solution used and the implementation scenario. If encryption is implemented with hardware support, then performance loss is less than in a software-based solution.
- Emergency guidelines for application errors caused by the user or by hardware problems

  Encryption is only performed for individual users. In other words, procedures for encryption recovery or data recovery must be used to ensure that encryption does not make it impossible to access company data. These procedures are also relevant, for example, if users delete the encryption key or if hardware problems prevent encryption for normal operation. The corresponding emergency mechanisms, procedures, and guidelines must therefore be available, planned, and implemented.
- Saving encrypted data

You must decide whether to save data in encrypted or unencrypted form. If you save in encrypted form, you must also ensure that the corresponding encryption keys are also saved so that you can decrypt the data again.

There are several options for data encryption in the mobile client context in SAP CRM. They have the following properties:

- You perform encryption at the operating system level or at a lower level
- You perform encryption for individual files or all data

The following solutions are currently available:

- File encryption using the encrypting file system (EFS)
- Encryption of virtual hard drives
- Hard-drive encryption

  In hard-drive encryption, the entire hard drive is encrypted. You must even specify a password for the boot process to decrypt and encrypt data again. Hard-drive encryption is available both as a software-based solution and as a hardware solution.

Note

Some manufacturers provide a hard disk drive (HDD) password to protect the hard drive. However, HDD passwords are used to merely restrict access to the hard drive controller. The data itself is not encrypted.

File Encryption Using the Encrypting File System (EFS)

In Windows 2000 and higher releases, Microsoft provides the option to encrypt individual files using software encryption. This makes is possible to encrypt the local CRM database. EFS is available as standard in Windows 2000 and higher releases.

Note

Products from other manufacturers also provide data encryption. This document lists only EFS because it is integrated with Windows.

To use EFS data encryption in the mobile client scenario in SAP CRM, you must first configure a Microsoft SQL server so that it runs on a dedicated user account. The CRM database files can then be encrypted for this user account.

Encryption must be activated in the selected user account. To do this, an administrator can log on interactively using the SQL server account and activate encryption for the database files.

Recommendation

We recommend that you combine all CRM-specific database files into a subdirectory and then flag this directory for encryption. Encryption key creation and management is performed automatically by Windows. This solution means that you need not run a Windows public-key infrastructure (PKI), although this is still possible if required. The encryption keys are kept in a user profile and can be entered using the normal backup procedure.

To ensure that only the SQL server account has access to these files, the access rights must be adjusted accordingly. These actions can also run automatically, controlled by scripts. To do this, you can use the commands `runas`, `cacls`, and `cipher`.

Since the Microsoft SQL server runs as a service, the user right *Log on as a service* must also be assigned to the SQL server account. This is done automatically if the corresponding account is entered in service administration.

If encryption-related problems occur, the machine can still perform most operations. Only applications that access encrypted data cannot operate correctly. In the CRM scenario, for example, the CRM application would no longer function correctly, but other computer functions, such as e-mail, can still be used.

Remember the following points:

- In Windows 2000 and higher releases, a domain account must be used as the SQL server account. Otherwise, an attacker can reset the password using the administrator account. The attacker can then log on to the account and decrypt the database files.
- Additional rights must be assigned to the SQL server account or they must be included in the local administrators group. We do not recommend the latter, however, as this would compromise the SQL server and could provide administration rights to an attacker.
- To prevent someone from logging on to the SQL server interactively after the initial encryption of the database files, the right to interactive logon must be removed from the account (user right: *Deny local logon*).
- The SQL server password saved in the registry database must not be stored in plain text because it could be used to access the encrypted data using the local SQL server.
- When using EFS, it is not possible to encrypt the swap file (disk space set aside for virtual memory) or the hibernation file (suspend to disk).
- The operating system cannot be encrypted.

Advantages of This Solution

- Software solution, no additional hardware required
- No additional costs
- No installation necessary
- Only the required files are encrypted
- Integrated with operating system (no compatibility problems)
- No PKI required
- Encryption key creation and administration is automated using Windows
- Encryption problems only affect applications that access encrypted data

Disadvantages of This Solution

- Configuration required
- Encryption must be activated explicitly for all files requiring protection
- The computer must run in a domain to use a domain account
- Data security depends on the operating system configuration (for example, protection of selected account on which SQL service runs, password quality, and user rights)
- Memory images are not protected
- The operating system is not encrypted
- You may be forced to accept lower performance than for a hardware-supported procedure

Encryption of Virtual Hard Drives

Unlike encryption of individual files, this solution allows encryption of all data that is copied to a virtual hard drive. The virtual hard drive is represented by a file saved in your file system, which can be connected as a separate drive using a special driver. The advantage of this solution is that all the data on the virtual hard drive is always encrypted. This type of encryption is called software encryption.

Unlike encryption of individual files, encryption of virtual hard drives allows you to encrypt the entire file hierarchy on the virtual hard drive. To do this, the correct software must be installed. The encrypted virtual drive is typically represented by a file in the computer's normal file system. The content of this file is always encrypted. When the file is connected as a drive, you enter a password, which is then used to encrypt and decrypt the data when the virtual drive is accessed.

In the mobile client scenario in SAP CRM, CRM database files could be stored on an encrypted virtual drive. Depending on the product, the encrypted hard drive is either connected automatically when the user logs on, or it must be activated manually. The virtual drive can also be used to save other sensitive data.

One advantage of this solution versus the encrypting file system (EFS) file encryption is that security of the data that is encrypted using EFS depends exclusively on the encryption software and the quality of the selected encryption password. An attacker who succeeds in getting past the operating system's access protection can then view the plain text data.

When selecting a product, make sure that the encryption product can also encrypt a virtual drive for several users. This is important because the CRM database may be accessed by several users, depending on the scenario. Access rights to the file that implements the virtual drive must be configured so that it can be accessed by all authorized users.

Encryption key generation and administration is performed within the encryption product. Depending on the range of functions, the product is also provided with its own public-key infrastructure (PKI), which must be installed and managed accordingly. Before or during initial operation, the keys must therefore be created either by the users themselves or by an administrator. Administration and backup of the keys must therefore be planned.

> Note
>
> When using encrypted virtual hard drives, it is not possible to encrypt the swap file (disk space set aside for virtual memory) or the hibernation file (suspend to disk). The operating system also cannot be installed on an encrypted virtual hard drive.
>
> Like file encryption, any encryption-related problems only affect the applications that access data saved on the encrypted virtual drive. The remaining computer functions are not affected.

Advantages of This Solution

- Software solution, no additional hardware required
- Data security independent of the operating system configuration
- All data on the virtual hard drive is always encrypted
- No access to plain text data even after the operating system has been compromised
- Encryption problems only affect applications that access encrypted data

Disadvantages of This Solution

- Installation of additional software required
- License costs for encryption software
- Files must be saved explicitly to the encrypted virtual drive
- Depending on the CRM scenario, the product must support encryption for several users
- Key generation and administration (including backup) must be planned separately
- A separate PKI must be used, depending on the product
- Memory images are not protected
- The operating system is not encrypted
- You may be forced to accept lower performance than for a hardware-supported procedure

Hard Drive Encryption (Software)

Encryption of the entire hard drive for a computer protects all the data on the hard drive equally. After installation, the encryption software starts during the boot process before the operating system. A password (used for decrypting and encrypting data) must be entered before all the data on the hard drive can be decrypted. This means that if the hard drive is stolen and accessed with a disk editor, the attacker can only access the encrypted data and not the plain text data.

This process can also be used in the CRM scenario because all the relevant data would also be covered by the encryption. In scenarios where several people are sharing a single CRM mobile client computer, make sure that the product used can also be operated for several users. Hard drive encryption products may also provide a preboot public-key infrastructure (PKI) that enables access to the encrypted disk (that is, access to the computers protected with the product). This PKI must then be installed and managed.

Compared to file encryption and virtual drive encryption, hard drive encryption provides general, all-around protection for all saved data. However, file encryption and virtual drive encryption place somewhat increased organizational and technical demands on an organization. In addition, encryption problems always affect the entire computer because the operating system is also encrypted.

Full encryption of the hard drive also protects the swap files. Standby mode (suspend to RAM) is typically supported by these products without any problems. Some products, however, might not support hibernation mode (suspend to disk), preventing you from using it. Where one or both of the suspend modes are supported, the password must be entered again when the computer starts up.

Advantages of This Solution

- Software solution, no additional hardware required
- All data on the hard drive is protected equally
- Security independent of operating system and its configuration
- The entire operating system (including the swap files) is encrypted

Disadvantages of This Solution

- Installation of additional software required
- License costs for encryption software
- Depending on the product, hibernation mode may not be supported (cannot be used)
- Increased technical and organizational demands
- A separate PKI must be installed, depending on the product
- When encryption-related problems occur, the computer can no longer be used
- You may be forced to accept lower performance than for a hardware-supported procedure

Hard Drive Encryption (Software and Hardware)

Besides fully software-based hard drive encryption, hardware can also be used to support encryption mechanisms. There are two main types of hardware support:

- Encryption of data using special hardware
- Hardware used to store the encryption keys

Only the first type is likely to provide improved performance because the second type still uses software to encrypt the data. Whether hardware encryption actually provides better performance than software encryption depends, to a large extent, on the technology used. If you are using a high-performance encryption chip that is well-integrated with the computer hardware (high level of data throughput), then you should experience a relatively small loss of performance.

Procedures that simply store the encryption key or user identities on separate hardware (such as smart cards or USB tokens) provide increased system access security because you need hardware as well as the password to access the system. This also means that if the hardware is lost, the computer can no longer be accessed. Of course, this is also true in the event of encryption-related problems. You therefore need to plan and execute emergency mechanisms and procedures. These must also be supported by the encryption product.

A product-specific public-key infrastructure (PKI) must also be used and managed.

Advantages of This Solution

- Depending on the implementation, better performance than with software solutions (hardware encryption)
- Depending on the implementation, greater security because physical possession of the hardware is required (keys/identities saved on the hardware)
- All data on the hard drive is protected equally
- Security independent of operating system and its configuration
- The entire operating system (including the swap files) is encrypted

Disadvantages of This Solution

- Installation of additional software required
- Installation of additional hardware required
- License costs for encryption product
- Depending on the product, hibernation mode may not be supported (cannot be used)
- Increased technical and organizational demands
- A separate PKI must be installed, depending on the product
- When encryption-related problems occur, the computer can no longer be used
- Performance depends on the product to a great extent

➡ Recommendation

We recommend that you encrypt the hard disk, because any kind of encryption is better than none at all. You must, however, evaluate the available options and pick the mechanism for encrypting the hard disk that best suits your application areas and requirements.

Checklist

Table 295

Feature	Check	How to Check
Hard disk encryption	Does the recommendation fit your scenario?	Select the type of encryption: File encryption using the encrypting file system (EFS), encryption of virtual hard drives, or hard drive encryption. Installation and usage of hard disk encryption.

5.2 SAP Mobile Service

SAP Mobile Service is a key functional area of SAP Customer Relationship Management (SAP CRM) that supports field service technicians who use offline mobile devices to access CRM data. The security information described in

SAP Mobile Sales [page 223] also applies to SAP Mobile Service. The underlying technology and integration paradigm to the CRM server are the same.

5.3 Mobile Client Synchronization

This section describes the security aspects associated with synchronization of data between the mobile client and the CRM server that is performed using the communication station.

Important SAP Notes

Table 296

SAP Note Number	Title	Comment
519995	Communication station: minimum authorizations	This SAP Note explains the minimum authorizations required to log on and work with SAP CRM.
618527	Business document (BDoc) type messages rejected due to missing authorizations	This SAP Note explains how to proceed in the following situations: • The remote function call (RFC) user on the communication station does not have complete authorizations (SAP_ALL). • The incoming queue is automatically carried out by another user who does not have the required authorizations.

User Administration and Authentication

User Management

Synchronization of data between the mobile client and the CRM server involves two types of users:

- Windows domain user to connect the mobile client to the communication station
- SAP ERP user to connect the communication station to the CRM server

Users

Table 297

System	User	Delivered?	Type	More Information
SAP CRM	RFC users for the internal logical connection `SAPCRM_MW_RR_*`	No	Communication	See the Customizing documentation
Communication station	RFC user to the CRM server	No	Communication	See the *Communication Station Installation Guide*
Mobile client	RFC user to the CRM server	No	Communication	N/A

User Management Tools

Table 298

Tool	Description
Windows user management	Tool provided by the Windows operating system

At the customer site, the Windows NT administrator must create users for mobile clients.

> **Note**
>
> One Windows user must be created for each mobile client.

The individual users are required to connect the mobile client to SAP CRM mobile transfer 5.2 on the communication station.

There is one technical user for each destination on the communication station. The SAP ERP user information is stored in the registry in an encrypted form on the communication station. Subsequently, this information is used to log on to the ERP server.

Authorizations

SAP CRM mobile transfer 5.2, which is a COM+ component, is installed along with the communication station. The following default roles are delivered along with this component:

- Administrator

  Used to change the technical settings of the component. In addition, you can create new users under the user role.

  > **Note**
  >
  > Customers are not required to create any new roles. However, customers can create new users by using the administrator role.

- User

  Allows mobile client users to access the component.

In addition, you can execute certain tasks or define access to different objects related to the mobile client by using the *Administration Console* (`SMOEAC`) transaction. The following table lists the standard roles in the SAP standard system, all of which authorize users to view sites:

Table 299

Role	Description
`SAP_CRM_MWAC_ADMIN_ALL`	Administration Console – Full authorizations
`SAP_CRM_MWAC_EMPL_CHANGE`	Administration Console – Maintenance of employees
`SAP_CRM_MWAC_EMPL_DISPLAY`	Administration Console – Display of employees
`SAP_CRM_MWAC_GROUP_CHANGE`	Administration Console – Maintenance of organizations
`SAP_CRM_MWAC_GROUP_DISPLAY`	Administration Console – Display of organizations
`SAP_CRM_MWAC_ILTP_CHANGE`	Administration Console – Maintenance of interlinkages
`SAP_CRM_MWAC_ILTP_DISPLAY`	Administration Console – Display of interlinkages
`SAP_CRM_MWAC_PUBL_CHANGE`	Administration Console – Maintenance of publications

Role	Description
SAP_CRM_MWAC_PUBL_DISPLAY	Administration Console – Display of publications
SAP_CRM_MWAC_REPOBJ_CHANGE	Administration Console – Maintenance of replication objects
SAP_CRM_MWAC_REPOBJ_DISPLAY	Administration Console – Display of replication objects
SAP_CRM_MWAC_SITE_CHANGE	Administration Console – Maintenance of sites
SAP_CRM_MWAC_SITE_DISPLAY	Administration Console – Display of sites
SAP_CRM_MWAC_SITE_INDIRECT	Authorization to start the indirect assignment of subscriptions: *Site Administration* (transaction SMOEIND)
SAP_CRM_MWAC_SITE_EXTRACT	Authorization to start extracts through the Administration Console: *Site Administration* (transaction SMOEIND)

Roles Related to the Subscription Generator

Table 300

Role	Description
SAP_CRM_MWAC_SUBAGENT_CHANGE	Administration Console – Maintenance of subscription agent
SAP_CRM_MWAC_SUBAGENT_DISPLAY	Administration Console – Display of subscription agent
SAP_CRM_MWAC_SUBSCR_CHANGE	Administration Console – Maintenance of subscriptions
SAP_CRM_MWAC_SUBSCR_DISPLAY	Administration Console – Display of subscriptions

R & R Queue Administration (Transaction SMOHQUEUE)

The authorization object is CRM_MW_RR.

Recommendation

You must have at least two profiles:

- Standard users: display only (Activity = 03)
- Power users: display, delete entries, and operate queues (Activity = 03+06+16)

Network and Communication Security

The following figure shows the system landscape of SAP CRM in the mobile scenario:

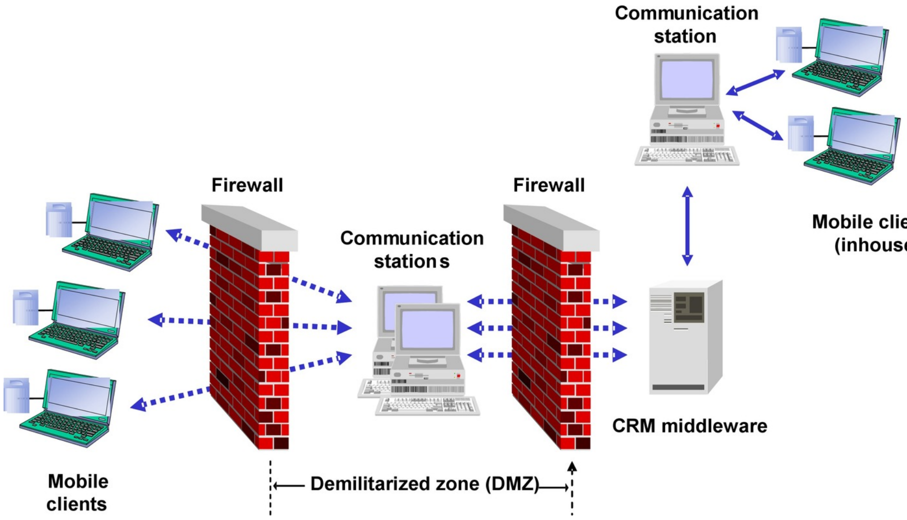


Figure 23: System Landscape — Mobile Scenario

The landscape consists of the following:

- One or more SAP ERP systems that operate as back-end servers. These SAP ERP systems are based on SAP NetWeaver Application Server (SAP NetWeaver AS).
- A CRM server that is based on a database in addition to the SAP NetWeaver AS. The CRM server also includes the middleware broker in SAP CRM.
- One or more communication stations that connect to the CRM server. The communication station is a system that is based on Windows 2000 or a higher release, with a Microsoft Transaction Server (MTS) (or COM+) infrastructure.
- Mobile clients that connect to one of the communication stations.
- Between the mobile clients and the communication station, a remote access server (RAS) or Microsoft Internet Information Server (IIS)-based Web server might exist. However, these instances and the communication station and SAP CRM might physically exist on the same machine.

> **Note**
>
> In a typical installation, security walls between some of these components may be required. This can be achieved using firewalls and security settings. For more information, see the *Security Settings for DCOM Connections* section below.
>
> Setting up connections between the CRM mobile clients, communication stations, and various SAP systems can be a complicated process in large organizations due to firewalls and network security policies, which require more detailed knowledge about the necessary network connections.

Communication Security Zones

Table 301

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Mobile client and communication station	DCOM	Binary	See security-related documentation under ▶ *MSDN Home* › *MSDN Library* › *Win32 and COM*

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
			Development > *Component Development* .
Communication station and SAP ERP systems	See the documentation for SAP connector for Microsoft .NET on SAP Service Marketplace at service.sap.com/connectors .		

Security Settings for RFC Connections

These connections are configured as RFC destinations on each system. To configure these destinations, you use the *Configuration of RFC Connections* (`SM59`) transaction within SAP NetWeaver AS. On the communication station, use `QmtCnfg.exe` to define the RFC destinations.

> Note
>
> It is useful to set up firewalls between all of these nodes. In many cases, there is at least one firewall separating the communication station from the other more critical instances, the SAP ERP systems, and the CRM server.

Security Settings for DCOM Connections

DCOM uses the following ports during communication:

- Fixed port 135 (TCP or UDP)

  Must be opened in the firewall all the time and cannot be reconfigured.

  While DCOM allows the usage of both TCP and UDP, the UDP packets can be spoofed easily and therefore represents a security risk. We recommend the use of TCP even though it is slower than UDP.

- Dynamically assigned port

  In the standard configuration, this port is allocated in the range `1024–65535`.

  Dynamic allocation of this port prevents conflicts with other applications. However, configuring a firewall is complicated. Therefore, you must restrict the port range that DCOM uses on the communication station to ensure that only ports opened within the firewall are used.

  > Note
  >
  > You must perform this activity only on the communication station and not on the clients.

  To do this, use `regedt32.exe` on the communication station (not `regedit.exe`), navigate to the `HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet` registry key, and enter or change the following named values:

  Table 302

Ports	This is a multiline entry. You can enter a single port or a port range (for example, `3000–4000`) on every line.
PortsInternetAvailable	Value must be `Y`
UseInternetPorts	Value must be `Y`

  For more information, see the Microsoft paper *Using Distributed COM with Firewalls* at msdn2.microsoft.com/en-us/library/ms809327 .

  Subsequently, you must permit all incoming traffic using the configured port range and single port `135`.

> Note
>
> Some firewalls allow IP address translations. However, this does not work with DCOM connections. The client must be able to connect to the server through its actual IP address.
>
> You can view the active DCOM settings directly by using the `QmtCnfg.exe` diagnostic tool on the client and the communication station. You can find the `QmtCnfg.exe` in the `<installation directory>\mobile\bin` directory on the client and the `<installation directory>\rfcsdk\crm` directory on the communication station.

Network Security

To allow the mobile client users to use mobile transfer 5.2 in SAP CRM, the following settings must be made on the communication station:

1. Log on to the communication station.
2. Choose *Start* > *Settings* > *Control Panel*.
3. Choose *Administrative Tools* > *Component Services*.
4. Choose *Console Root* > *Component Services* > *Computers* > *My Computer* > *Com+ Applications*.
5. Choose *SAP CRM Mobile Transfer 5.2* > *Roles* > *User* > *Users*.
6. Right-click on *Users* and choose *New* > *User*.
7. Add all the Windows users or Windows user groups specified in the domain that have access to the component.

   > Note
   >
   > Authentication using local users on the mobile client is not supported.
   >
   > If the mobile clients and the communication station are on different NT domains, then a trust relationship must be established for these settings to be effective.

8. Reboot the communication station.

   > Note
   >
   > The communication occurs through DCOM, which allows you to choose from a range of ports.

You can set up the network infrastructure by using any of the following methods:

Intranet Access

In an intranet scenario, the recommended way to set up the network infrastructure is as follows:

- Ensure that the mobile clients and the communication station share access to the same Windows domain controller.
- Activate security on the communication station package `SAP CRM Mobile Transfer 5.2` and the `DOTNET.TransSrv` component by using the *Component Services* in the *Administrative Tools* part of the *Control Panel*. After installation, this is the default setting.
- Configure the appropriate roles and user groups. You can restrict access to the transfer service only to the group of users using mobile clients. However, this is not mandatory because the transfer service itself checks for registered clients and allows only pass-through calls from clients that are known to the site administration of the administration console.

- You may want to place the CRM server and SAP ERP systems in a separate and isolated domain. In addition, you may want to place a firewall between the communication stations, and the CRM server and SAP ERP systems to allow at least incoming traffic to use the `33xx` ports.
- If you must provide firewalls between mobile clients and their communication station, ensure that you switch to TCP/IP as the preferred DCOM transport protocol on all sides with the necessary ports opened.
- You can choose to use any authentication level for the authentication: wire encryption or packet integration checks by configuring the appropriate parameter for the transfer service component `DOTNET.TransSrv`.

Extranet Access

Extranet access is possible either using a virtual private network (VPN) or direct dial-up.

> **Recommendation**
>
> Use VPN for extranet access of mobile clients to the communication station. All the settings mentioned for intranet access are applicable after setting up the VPN.
>
> The VPN connection must be based on HTTPS connectivity rather than HTTP.

Direct dial-up access is also possible, though not recommended.

Direct Dial-Up Access

The preferred method to set up the infrastructure for dial-up users is to allow the mobile clients to log on to the network during dial-up and ensure that the dial-up clients and their communication station use (or have access to) the same Windows domain. Subsequently, perform the same steps as described for intranet clients.

If, however, you cannot allow the clients to log on to the network or if the clients and their communication station must not exist in the same Windows domain (perhaps, because there is a firewall between them), you can use the following method. Create local users on the communication station with the same name and passwords as for the mobile clients and assign these users to the roles configured for access to the transfer service. This is not a simple task. Therefore, we recommend that you turn off DCOM security or use the Internet scenario.

Communication Destinations

The communication station and the CRM server communicate through RFC calls. Therefore, you must create an RFC destination by using `QmtCnfg.exe` available on the communication station.

Table 303

Destination	Delivered?	Type	User, Authorizations	Description
AC-NET4ABAP: Mobile Client User Administration	No	TCP/IP destination	To create an RFC user, see Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Create RFC Users* ◀. **Recommendation** Assign minimum authorizations to this user.	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Define RFC Destinations* ◀. See the *Communication Station Installation Guide* on SAP Service Marketplace at service.sap.com/instguides.

Destination	Delivered?	Type	User, Authorizations	Description
			For more information, see SAP Note 519995.	

Data Storage Security

The data recorded by sales representatives is stored in the user database of the mobile client. This data is stored when the sales representative performs an activity on the mobile client, such as creating a sales order. Subsequently, this data is synchronized with SAP CRM through the communication station and stored in the consolidated database (CDB) on the CRM server.

During synchronization, the data stays in the queues that are available both on the CRM server and mobile client. The queues are further classified into inbound and outbound queues that sequentially send and receive data from the mobile client and the CRM server respectively.

Trace and Log Files

The runtime information associated with data synchronization between the mobile client and the CRM server is logged in the `TransferService.Log` file that is created both in the mobile client and the communication station.

> ➡ Recommendation
>
> Set the trace level to the minimum value to ensure that the minimum amount of information is logged in the log file.

In mobile system maintenance, you can maintain the security-related events that must be logged. These events are:

- Successful logon and logoff
- Failed logon
- Change of password
- Change in settings for integration of SAP Mobile Sales with SAP Mobile Time and Travel

In SAP CRM, you can now lock or unlock a user’s access to mobile applications. When the mobile client synchronizes with the server, this information is available on the mobile client. The lock and unlock settings are then used on the next logon attempt by this user.

Passwords are case-sensitive and are enforced by the system.

Single sign-on information for the integration of SAP Mobile Sales with SAP Mobile Time and Travel is encrypted for protection.

6 Component-Specific Guidelines: Web Channel Enablement

Web Channel Enablement scenarios consist of ABAP functions on the CRM or ERP server and Java-based functions on the Java application server (AS Java). The Java-based applications running on the AS Java provide the user interface to functions on the CRM or ERP server.

This section provides specific security information for the Web channel function for the following:

- The e-commerce application in SAP CRM
- The e-commerce application in SAP ERP (mostly Web applications)
- The e-service application in SAP CRM

The term Web Channel Enablement comprises all Web channel applications.

The security-relevant topics for dependent components, such as the AS Java, are described in detail in the following corresponding security guides.

Table 304

Application	Guide	Most-Relevant Sections or Specific Restrictions
SAP NetWeaver	Security guides for SAP NetWeaver on SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform	How to configure secure sockets layer (SSL) How to install secure network communication (SNC)
Partner channel management	Access control engine (ACE)	N/A
Web channel	ACE	N/A

Why Is Security Necessary?

SAP CRM helps you with Web Channel Enablement, which allows you to do your business-to-business (B2B) or business-to-consumer (B2C) business over the Internet. Hence, security is important because any business-related information can be accessed and your application can be the target of many different attack scenarios.

The following table provides an overview of some attack scenarios and references to subsections that detail how to protect your application:

Attack Scenarios

Table 305

Attack Type	Description	Relevant Subsections
Broken access control	Once authenticated, users are not properly granted access or restricted in the activities they can perform.	*User Administration and Authentication* *Data Storage Security* *Other Security-Relevant Information*
Broken authentication and session management	The account credentials and session tokens may not be properly protected. As a result, attackers can overcome authentication	*Network and Communication Security*

Attack Type	Description	Relevant Subsections
	restrictions to access passwords, keys, session cookies, or other tokens and assume other users' identities.	
Configuration management that is not secure	Security-relevant setting is on in the production environment	*Restricting Access to Technical Administration of Web Channel Applications*
Storage that is not secure	Data stored in the files is not protected accordingly	*Data Storage Security*
Distributed denial-of-service (DDOS)	DDOS attacks	*Other Security-Relevant Information*

Important SAP Notes

Table 306

SAP Note Number	Short Text	Comment
715371	Composite Security Note: AS Java 6.30/6.40	This note provides information related to the security of the AS Java.
891659	Composite Security Note AS Java 7.00	This note provides information related to the security of the AS Java 7.00
1503236	Application Configuration based on J2EE Security Settings	The note provides information on how to configure Web channel applications with regard to the J2EE Security Settings
1492234	No SessionIDRegeneration in CRM Web Channel B2C/B2B Scenario	The note provides information on how to configure Web channel applications to enable a session ID regeneration (security session)
894446	ECO: Using UME logon application in SAP e-commerce	The note provides information on how to configure the usage of the UME Logon application

For more information on security-relevant SAP Hot News and SAP Notes, see service.sap.com/securitynotes

Technical System Landscape

The figure below shows an overview of the technical system landscape for the SAP E-Commerce Web applications:

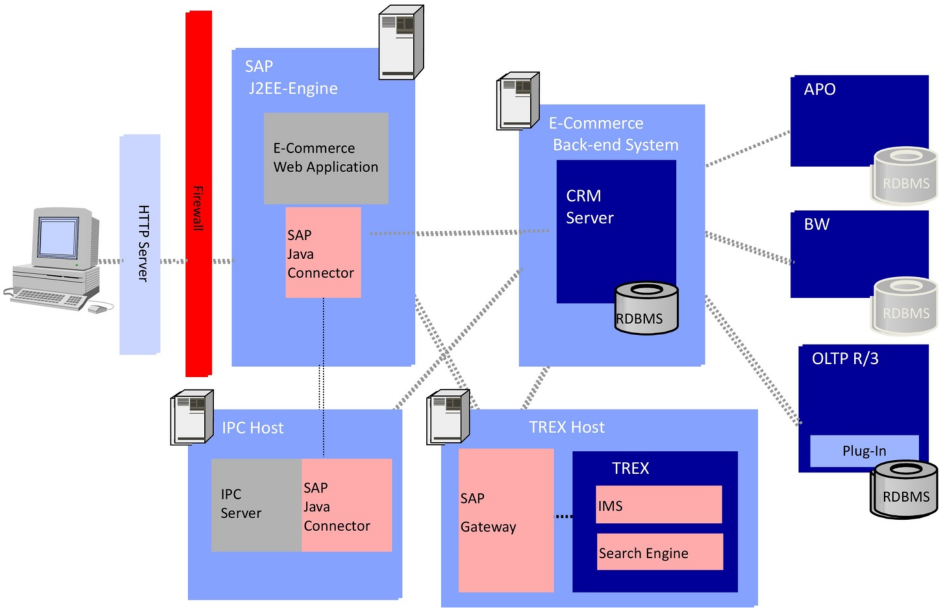


Figure 24: Technical System Landscape for SAP E-Commerce

For more information about the technical system landscape, see the following table:

Table 307

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace or SDN
Technical Description for CRM Web channeland the underlying components such as SAP NetWeaver	Master Guide for SAP CRM	service.sap.com/instguides
High Availability	High Availability for SAP Solutions	sdn.sap.com/irj/sdn/ha
Technical Landscape Design	See applicable documents	sdn.sap.com/irj/sdn/landscapedesign
Security	See applicable documents	sdn.sap.com/irj/sdn/security

Security Aspects of Data, Data Flow and Processes

The figure below shows an overview of the security aspects of data, data flow, and processes for the SAP E-Commerce web applications.

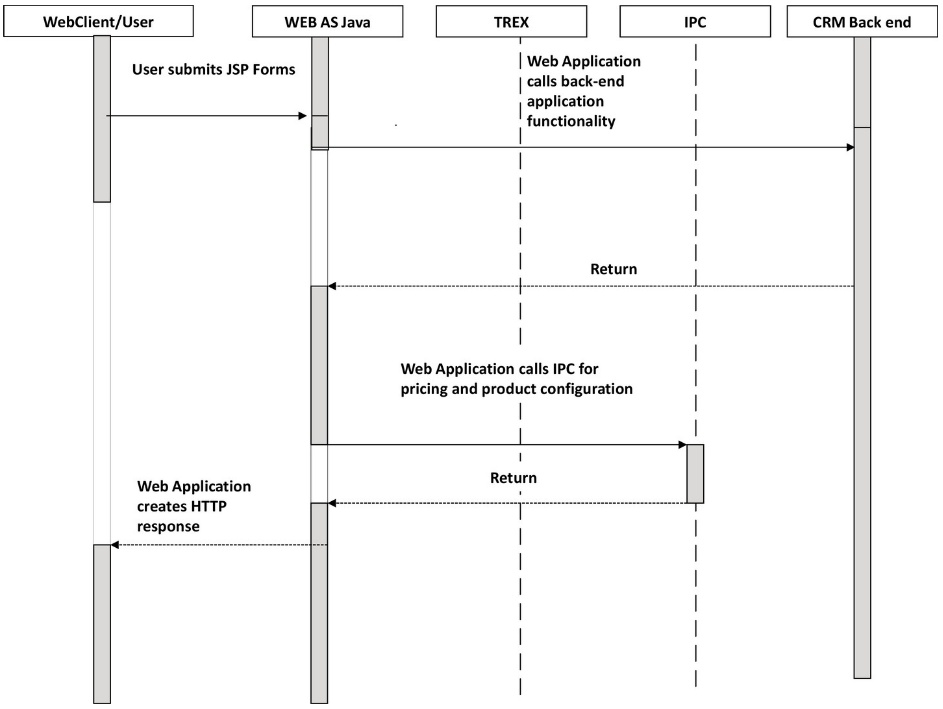

WebClient/User
WEB AS Java
TREX
IPC
CRM Back end
User submits JSP Forms
Web Application calls back-end application functionality
Return
Web Application calls IPC for pricing and product configuration
Return
Web Application creates HTTP response

Figure 25: Overview of Security Aspects of SAP E-Commerce Web Applications

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

Table 308

Step	Description	Security Measure
1	User submits HTML form	User Types • Dialog user for functionality that needs authentication • Service user for anonymous functionality such as the product catalog in B2C Communication Protocol HTTPs is recommended
2	Web application calls back-end application functionality via SAP Java Connector (RFC)	SNC for the RFC connection
3	Web application calls IPC for pricing and/or product configuration	SNC for the RFC connection

User Administration and Authentication

The type of user administration differs depending on whether you use Web Channel Enablement in SAP CRM or SAP ERP.

This section lists the tools for user management, types of required users, and standard users that are delivered with Web Channel Enablement.

Note

Web Channel Enablement uses the SU01 user concept.

As of SAP NetWeaver 701, the *Maintain Internet user* (SU05) transaction is no longer available, so it is no longer possible to create and maintain SU05 Internet users. It is possible to migrate SU05 users to SU01 users. For more information, see SAP Note 1324366 and SAP Note 593439.

Since the e-commerce application could run on ERP systems based on SAP NetWeaver releases earlier than the 701 release, the *Maintain Internet user* (SU05) transaction is still mentioned in this guide. We recommend that you use the SU01 user concept.

User Management

User Management Tools for all Web Channel Scenarios

Table 309

Tool	Description	Prerequisites
SAP NetWeaver Application Server Java (SAP NetWeaver AS Java) user management using the SAP NetWeaver Administrator	Access to administration pages that are part of every Web channel application, is controlled using SAP NetWeaver AS Java security.	Automatically activated after deploying the Web channel applications
Web-based user management	For information about configuration, see SAP Solution Manager.	Only applicable for B2B users with user type that can be maintained by using the *User Maintenance* (SU01) transaction. The application uses the ABAP user management application programming interface (API). For more information, see SAP Solution Manager.
Web-based user management using the SAP User Management Engine (UME)	For more information, see the user management engine documentation and SAP Note 891151.	The application uses the ABAP user management API and the user management engine API. The user management engine logon function is integrated in all Web channel applications.
Internet User self-service	User self-registration and self-maintenance function	Only applicable for business-to-consumer (B2C) applications. The self-service functions use the ABAP user management API for SU01 or SU05 users.

User Management Tools: E-Commerce for SAP ERP

Table 310

Tool	Description	Prerequisites
User and role maintenance with SAP NetWeaver AS ABAP (Transactions `SU01`, `PFCG`)	User and Role Administration of Application Server ABAP.	Possible for B2B, B2C, shop management, and user management applications. For information about the logon configurations for SAP E-Commerce, see SAP Solution Manager.
Maintain Internet user (transaction `SU05`)	For more information, see the documentation for the *Maintain Internet User* transaction. As of SAP NetWeaver 701, the *Maintain Internet user* (`SU05`) transaction is no longer available, so it is no longer possible to create and maintain `SU05` Internet users. We recommend that you use users that can be maintained using the *User Maintenance* (`SU01`) transaction.	Only possible for B2B and B2C applications. For information about the logon configurations for SAP E-Commerce, see SAP Solution Manager.

User Management Tools: Web Channel Enablement for SAP CRM

Table 311

Tool	Description	Prerequisites
User and role maintenance with SAP NetWeaver AS ABAP (Transactions `SU01`, `PFCG`)	User and Role Administration of Application Server ABAP.	Possible for B2B, B2C, Web-based user management, and shop management applications. For more information, see SAP Solution Manager.
Maintain Business Partner (transaction `BP`)	For more information, see SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Master Data* › *Business Partners*.	Only available on SAP GUI
CRM Web UI accounts	N/A	Only available in WebClient UI

User Types

The following users must be created for Web Channel Enablement:

User Types for All Web Channel Applications

Table 312

System	User	Delivered?	Type	Default Password	Description
SAP NetWeaver AS Java	Administrator	Yes (part of SAP NetWeaver	User administered on	As defined during installation of SAP	This user can be used to enter the Web channel applications administration pages. For more

System	User	Delivered?	Type	Default Password	Description
		AS Java installation)	SAP NetWeaver AS Java	NetWeaver AS Java	information, see *Extended Configuration Management (XCM)* in SAP Solution Manager. We recommend that you create a new user with fewer rights for administration of Web channel applications instead of using the SAP NetWeaver AS Java administrator (see next row).
SAP NetWeaver AS Java	Isaadmin	No	User administered on SAP NetWeaver AS Java	No	We recommend that you create this user after installing SAP NetWeaver AS Java (together with the SAP CRM Java applications). For more information, see below for *Restricting Access to Web Channel Administration Pages from the Internet*, under *Other Security-Relevant Information*.

User Types for E-Commerce for SAP ERP

Table 313

System	User	Delivered?	Type	Default Password	Description
SAP ERP	Anonymous user for stateless connection	No	Service user created using the *User Maintenance* (`SU01`) transaction	No	User for establishing the stateless connection between SAP ERP and SAP E-Commerce. This user must be maintained in the application configuration administrator tool. For example, this user is used for determining the SAP ERP release before the SAP E-Commerce user logs on or for reading the SAP ERP catalog or for Customizing. We recommend that you use separate service users for each application, using the appropriate application service user role. For more information, see Authorizations [page 25].
SAP ERP	E-commerce user	No	Dialog user created using one of the user management tools mentioned above.	No	The user that logs on to SAP E-Commerce. The full-state SAP E-Commerce connection is established with it and sales documents are created using this connection. Only relevant if the logon type is `4, 7, 8`, or `9`. This corresponds to the application configuration settings

System	User	Delivered?	Type	Default Password	Description
					R3_SU01User, R3_SU01UserContactPerson, R3_SU01UserStandalone, or R3_SU01Customer_LoginEmail in component `usertype`. For more information, see SAP Solution Manager.
SAP ERP	E-commerce user	No	`SU05` user created using the *Maintain Internet User* (`SU05`) transaction (in case of B2B and B2C or the B2C self-registration)	No	The user that logs on to SAP E-Commerce. The full-state SAP E-Commerce connection is established with the anonymous user created using the *User Maintenance* (`SU01`) transaction. Only relevant if the logon type is `0`, `1`, or `2`. This corresponds to the Extended Configuration Management (XCM) settings R3_SU05Customer_LoginCustomerNo, R3_SU05Customer_LoginEmail, or R3_SU05ContactPerson_LoginContactPersonId in component `usertype`. For more information, see SAP Solution Manager.

User Types for CRM Web Channel Enablement and Partner Channel Management

Table 314

System	User	Delivered?	Type	Default Password	Description
SAP CRM	Service (anonymous) user for stateless connection	No	Service user created using the *User Maintenance* (`SU01`) transaction	No	User for establishing stateless connection between SAP CRM and Web Channel Enablement. We recommend that you use separate service users for each application, using the appropriate application service user role. For more information, see Authorizations [page 25].
SAP CRM	Web channel user	No	Dialog user created using one of the user management tools mentioned above	No	The user that logs on to Web channel. The full-state Web Channel Enablement connection is established with this user.

Additional User Types for CRM Web Channel B2C Application

Table 315

System	User	Delivered?	Type	Default Password	Description
SAP CRM	CRM user working as a call center agent	No	Dialog user created using the *User Maintenance* (`SU01`) transaction	No	A user with call center agent authorization who logs on to business-to-consumer (B2C) is able to act on behalf of a consumer.

User Data Synchronization

This topic describes how user data is synchronized with other systems. It also describes which user data information must be managed in different systems.

In some cases, it is necessary for the user data to be maintained in different systems to implement integrated scenarios. To synchronize the user data in different ABAP-based systems, the standard function of central user administration (CUA) is used. For more information, see the CUA documentation.

The synchronization of user data outside of the ABAP systems is realized through the user management engine (UME). In this case, the principle of double data maintenance is used. This means that data is maintained first in an ABAP back-end system (CRM or ERP system); the same user data is maintained later in the UME system.

The user data for business-to-business (B2B)-based Web Channel Enablement is maintained by the Web channel user management application. The support of CUA and UME for Web channel applications is supported only by this application.

Support of the User Management Engine (UME) and User Data Synchronization

The Web channel applications, B2B shop (all scenarios), and Web-based user management support UME and SAP NetWeaver Portal concurrently, as UME is included in SAP NetWeaver Portal.

The replication of user data between Web channel and UME occurs directly through UME-API, which runs on the same AS Java as Web channel. For more information, see SAP Note 891151.

Regarding synchronization of user data and user roles between Web channel user structure and UME user structure, a configuration file exists where this data is maintained. For more information, see SAP Note 891151.

Furthermore, e-commerce components provide an option to use a UME logon application. In such a case, UME provides an authentication service that is called before logging on to Web channel applications. After a successful authentication, UME creates a single sign-on (SSO) ticket that in turn is transmitted to the Web channel application. For more information, see the UME documentation.

> Note
>
> If the user storage of UME is connected to the same ABAP-based back end as the Web channel application, the replication between Web channel and UME must not be performed. In this case it is sufficient if the Web-based user management application creates only users based on `SU01` user ID. Check the value of the user type parameter in the XCM application configuration that is used.

Logon Processes

Since SAP CRM 5.0, most Web channel applications use one central logon module implementation. This logon module includes different logon procedures. The following are examples of logon procedures:

- Web channel logon

  This logon corresponds to the logon function of earlier releases of Web Channel Enablement. You use this for upgrade scenarios, for example, for support when logging on with an SU01 user alias.
- UME logon

  This logon is based on the UME logon application that is a part of the core services of SAP J2EE Engine 6.30 (and higher). Before the Web channel application is processed, UME provides its authentication services. Other logon methods are available with UME logon service, such as SAP logon tickets (SSO2) or X.509 digital certificates.

  For more information, see the UME documentation. For more information about Web-channel-specific settings, see SAP Note 894446. We recommend that you use the UME logon procedure as a default.

Integration into Single Sign-On Environments

Apart from the logon procedure that is used, all Web channel applications that have the central logon module accept SAP logon tickets (SSO2) as the logon procedure.

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. SAP logon tickets are only created at authentication if the UME logon is used.

Authorizations

The Web Channel Enablement uses the authorization concept provided by the SAP NetWeaver AS ABAP and AS Java. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP and SAP NetWeaver AS Security Guide Java also apply to the Web Channel applications. The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP and the User Management Engine's user administration console on the AS Java.

> Note
>
> For more information about creating roles, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security* › *Identity Management* .

Authorizations Based on User Roles

User Roles based on the UME are used for the Extended Configuration Management (XCM) of the Web Channel applications.

The following table lists the roles that are created on SAP NetWeaver AS Java for each Web channel application when the application is installed.

The Web channel application roles are visible using *Visual Administrator* › *Security Provider* › *Policy Configurations* › *Security Roles*

Authorizations Valid for All Web Channel Applications

Table 316

Role	Description
Isaadmin	Automatically assigned to the administrators group after installation. All users assigned to this role can enter the Web channel administrator area. This role is used by system administrators when configuring the Web application, for example, when using XCM. We recommend that you create a new user for Web channel administration and assign it to this role. This prevents Web channel application administrators from having full access to SAP NetWeaver AS Java.
Computing center management system (CCMS)	Automatically assigned to the administrators group. This role is only used internally by the application for reporting of version or configuration information to the central monitoring system. You do not have to make any changes.
Isasupport	Automatically assigned to the `SAP_JAVA_SUPPORT` group after installation. If this is not the case, see SAP Note 1014383. All users assigned to this role can enter the Web channel administrator area in read-only mode. This role is used by SAP support when checking the Web application.

PFCG user roles are used for the Internet users and service users of the Web channel applications.

The following table lists the Web channel user roles that are in the back-end system. For each Web channel application, individual user roles for the Internet users and service users (anonymous users) are provided. For more information about roles and how to configure custom user roles, see SAP Solution Manager and SAP Note 1035065.

User Roles for SAP E-Commerce for SAP CRM

Standard SAP CRM roles generally use the following naming convention:

`SAP_CRM_ECO_<Component>_<Usertyp>_<Application>_<Appendix>`

- Component
  - ISA (Internet Sales)
  - ISE (Internet Service)
- Usertyp
  - WU (Internet or Web User)
  - TU (Service or Technical User)
- Application, for example
  - B2B
  - B2C
- Appendix
  - Document Authorizations, such as Full, Order,View
  - Additional Authorizations such as Loyalty, Auction

Examples:

- `SAP_CRM_ECO_ISA_WU_B2B_FULL`
- `SAP_CRM_ECO_ISA_TU_B2C`
- `SAP_CRM_ECO_ISA_WU_B2C_LOYALTY`

Table 317

Role	Description
SAP_CRM_ECO_ISA_WU_B2B_FULL	Business-to-business (B2B) with full document authorization
SAP_CRM_ECO_ISA_WU_B2B_ORDER	B2B with full order authorization and authorization to display sales order documents
SAP_CRM_ECO_ISA_WU_B2B_VIEW	B2B with authorization to display sales order documents
SAP_CRM_ECO_ISA_WU_B2B_AUCTION	Additional auction authorizations for B2B Internet users. If you are using auctions, you must also assign this role to your B2B users.
SAP_CRM_ECO_ISA_TU_B2B	B2B service (anonymous) user
SAP_CRM_ECO_ISA_TU_B2B_AUCTION	Additional auction authorizations for B2B service user. If you are using auctions, you must also assign this role to your B2B service user.
SAP_CRM_ECO_ISA_WU_B2C	Full business-to-consumer (B2C) authorization (when the user is logged on). This role is assigned to a reference user.
SAP_CRM_ECO_ISA_TU_B2C	B2C service (anonymous) user
SAP_CRM_ECO_ISA_TU_B2C_ORDER	Additional authorizations for usage of CRM orders as in Web Channel Enablement B2C. This is needed in the shop scenario for telco customer self service. In such a scenario, assign the roles SAP_CRM_ECO_ISA_TU_B2C and SAP_CRM_ECO_ISA_TU_B2C_ORDER to your technical user.
SAP_CRM_ECO_ISA_WU_EASYB2B	B2B authorizations for occasional users based on B2C-like Web application
SAP_CRM_ECO_ISA_TU_EASYB2B	Authorizations for service user of B2B for occasional users.
SAP_CRM_ECO_CALLCENTERAGENT	A user with call center agent authorization who logs on to B2C is able to act on behalf of a consumer.
SAP_CRM_ECO_ISA_TU_SHOPADMIN	Shop management service (anonymous) user
SAP_CRM_ECO_ISA_WU_SHOPADMIN	Full shop management authorization.
SAP_CRM_ECO_ISA_WU_BOB_FULL	Business-on-behalf (BOB) with full sales order document and quotation authorizations
SAP_CRM_ECO_ISA_TU_BOB	BOB service (anonymous) user
SAP_CRM_ECO_ISA_WU_HOM_FULL	Hosted order management with full authorization
SAP_CRM_ECO_ISA_WU_HOM_VIEW	Hosted order management with authorizations to display documents
SAP_CRM_ECO_ISA_TU_HOM	Hosted order management service (anonymous) user
SAP_CRM_ECO_ISA_WU_CSR	Authorizations for Internet users of the collaboritave showroom application
SAP_CRM_ECO_ISA_TU_CSR	Authorizations for service users of the collaborative showroom application
SAP_CRM_ECO_ISA_WU_USERADMIN	Authorizations for Internet users of the collaborative showroom application

Role	Description
SAP_CRM_ECO_ISA_WU_USERADMIN	Authorizations for service user of the collaborative showroom application
SAP_CRM_ECO_ISA_WU_USERADMIN	Full user administration authorization; this is the role for a superuser.
SAP_CRM_ECO_ISA_TU_USERADMIN	User administration service (anonymous) user
SAP_CRM_ECO_TU_AVW	An anonymous user for auctioning in a Web shop. Used in logon and background tasks like determining the winners for auctions.
SAP_CRM_ECO_AVW_WU_SELLER	Creates and manages auctions in auctioning in a Web shop.
SAP_CRM_ECO_AVW_WU_ADMIN	Configures the background tasks required for auction management process in auctioning in a Web shop.
SAP_CRM_ECO_ISA_TU_B2C_LOYALTY	Authorization for loyalty management anonymous user
SAP_CRM_ECO_ISA_WU_B2C_LOYALTY	Authorization for loyalty management user

The roles are single roles to enable an integration into composite roles for portal enabling.

User Roles for SAP E-Commerce for SAP ERP

For information about authorization roles relevant for SAP E-Commerce for SAP ERP, see SAP Solution Manager.

Standard SAP ERP roles generally use the following naming convention:

`SAP_ISA_<Application>_<Appendix>`

- Application, for example
  - B2B
  - B2C
- Appendix
  - Document Authorizations, such as Full, Order,View
  - Authorizations for Technical Users, such as RFC.

Table 318

Authorization Role in the Back End	Description
SAP_ISA_B2C_RFC	Role for the business-to-consumer (B2C) remote function call (RFC) user
SAP_ISA_B2C_FULL	Role for the B2C users created using the *User Maintenance* (SU01) transaction. To improve system performance, this role must be assigned to the reference user, not to users directly.
SAP_ISA_B2B_RFC	Role for the business-to-business (B2B) RFC user
SAP_ISA_B2B_VIEW	B2B, only view catalog and maintain templates
SAP_ISA_B2B_ORDER	B2B, create orders

Authorization Role in the Back End	Description
`SAP_ISA_B2B_FULL`	Full B2B authorizations
`SAP_ISA_BOB_FULL`	Full business-on-behalf (BOB) authorizations
`SAP_ISA_SHOPMGMT_RFC`	Shop management RFC user
`SAP_ISA_SHOPMGMT_FULL`	Full shop management authorizations
`SAP_ISA_UADM_RFC`	User management RFC user
`SAP_ISA_UADM_SUPERUSER`	User management: customer superuser that has authorizations to maintain users for his or her company

Partner Channel Management

In partner channel management, the roles are in the standard system, along with external services objects included in the user menu. The external service for the user interface (UI) provides a comprehensive list of all authorization objects used in a UI application. In addition, predefined values for authorization objects can also be defined. This method is used for applications relevant to partner channel management to assign authorization objects and their values to different roles. The list of external services assigned to a role can be viewed in the menu tab of a role, directly under the SAP NetWeaver Portal role node.

These external services are defined only for UI applications in the role. For applications or views in different roles, the authorizations are provided in the delivered roles.

With external services, the default values for authorizations are not automatically taken over by the profile generator. There is an intermediate step where the customers must copy the SAP standard values to the customer namespace and then change these values. You do this using transaction `SU24`. For more information about missing authorizations in generated profiles, see SAP Note 444686.

Authorizations Based on the Access Control Engine

The Access Control Engine (ACE) is another important step towards authorizations in partner channel management and Web Channel Enablement. The ACE is designed to help control user access, and is used with the ABAP authorization concept to help control user access to the applications and data. This means that you can, in addition to measures taken on other architecture levels, use application logic to define which users see which data, and whether those users have authorization to read, edit or delete that data. For more information, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *Basic Functions* > *CRM Access Control Engine* and the section Access Control Engine [page 324].

Take into account the additional security measures described in the section Security for Third-Party or Additional Products [page 39]. You could also consider alternative landscape topologies including, but not limited to, the set-up of separate SAP CRM instances for partner channel management scenarios and processes and Web Channel Enablement scenarios and processes. The chosen topology would, of course, depend on your security policies with regard to access of external parties to your business systems.

Currently the ACE checks run only in SAP CRM back end. To set up the ACE, the customers must go through certain steps, as defined in the ACE guide. In addition, customers can define their own rules and access rights to provide additional access control, based on their business requirements.

For more information, see Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* and SAP Note 941889.

Authorization Objects

The table below shows a selection of the special authorization objects that this application uses:

Table 319

Authorization Object	Short Text	Description
ECO_DOC_LP	E-commerce document authorizations	ECO_DOC_LP is the authorization object for granting Internet users access to different documents in the E-commerce Applications. You use the field value settings of this object to restrict access to the corresponding documents in the application. For example: If users have *Read Only* permission for sales orders (Doc. Type: *ORDR*), then the corresponding link for order creation in the application is not visible and nor can the activity be performed from the implementing Java Application.
ECO_DOC_BH	E-commerce document authorizations for dealer family	Specific to users in the business partner hierarchy scenarios. This object authorizes users to work on the behalf of the family (BP Hierarchy). If, for example, users are allowed to create orders for other members in the Family then, this authorization is required for this object. Implement this check only for users working on behalf of other members in the family. The profiles should only include this object for the scenarios where a user is allowed to work for multiple members in the business partner hierarchy. For more information on how to grant authorizations, see the documentation for ECO_DOC_LP.
S_RFC	Authorization Check for RFC Access	Authorization check for RFC access to program modules (for example, function group, function modules).
S_USER_PRO	User Master Maintenance: Authorization Profile	Authorization object, checked during authorization maintenance. This object controls the assignment of user profiles and is required in the user roles: ● B2C Service user

Authorization Object	Short Text	Description
		- Useradministration User (Superuser, Webshop Manager) to enable the assignment of profiles that belong to user roles
`S_USER_AGR`	Authorizations: Role Check	The authorization object is used to protect the roles. The roles are used to combine users in groups and to assign them different attributes, in particular transactions and authorization profiles. This object controls the assignment of user roles and is required in the user roles: - B2C Service User - Useradministration User (Superuser, Webshop Manager) to enable the assignment of user roles.
`S_USER_GRP`	User Master Maintenance: User Groups	Authorization object that is checked during user maintenance. The object is defined with the following two fields - User group This field can be used to set a user administrator for maintenance of one or more user groups when there is more than one user administrator. Every user must be assigned to a user group. Users that are not assigned to a group can be maintained by all user administrators. As of Release 4.6, users can be assigned to more than one group. Note that one group is marked as relevant for the authorization check. This is the group listed under the *Logon data* tab in the user maintenance transaction `SU01`. - Activity This field can be used to limit what the administrator is allowed to do with the authorization.
`S_USER_SYS`	User Master Maintenance: System for Central User Maintenance	Authorization object for central user administration (CUA). From one central system, users can be distributed in different child systems in

Authorization Object	Short Text	Description
		a system group. The system uses the object S_USER_SYS to check the child systems to which the user administrator can assign users. The authorization object is also checked when setting up the CUA.
S_USER_SAS	User Master Maintenance: System-Specific Assignments	Authorization object S_USER_SAS is checked in transactions SU01, SU10, PFCG, and PFUD when roles, profiles, and systems are assigned to users. It is a further development of the authorization objects S_USER_GRP, S_USER_AGR, S_USER_PRO, and S_USER_SYS, which were previously checked when authorizations were made. The checking of authorization object S_USER_SAS is activated using a Customizing switch. If this switch is not set, the previously used authorization objects are checked. To activate it, use transaction SM30 to create an entry in table PRGN_CUST with the ID CHECK_S_USER_SAS and the value YES.

Note

1. The authorization objects S_USER_PRO and S_USER_AGR **should only contain** user roles and user profiles required for Internet users of the Web Channel applications.

   Do not assign full authorization (value *) to the authorization fields *Role Name* and *Auth. Profile*.

   For B2C these are the user roles and user profiles that are assigned to the B2C Reference User. For the Web-based user management these are the user roles and their profiles that are maintained in the Web-based user management Customizing to enable an assignment in the Web-based user management application in *Customer Relationship Management* > *Web Channel* > *Basic Settings* > *Internet User* > *Web Based User Management* > *Set Up Roles for Web-Based user Management*)

   To raise the security level of the shipped roles, the authorization objects S_USER_AGR and S_USER_PRO are inactivated. Assign the roles and profiles that are used in your B2C and B2B scenarios to the authorization objects and activate the authorizations in the roles or the copies of the roles. For more information, see SAP Note 1521370.
2. The authorization objects S_USER_SYS and S_USER_SAS are only required when a Central User Administration is used. Consequently, the authorization objects are deactivated in the shipped roles as well. Activate the authorization objects and maintain proper authorization values if a CUA is used.

⚠ Caution

You cannot specify specific user groups for the creation of B2C or B2B Internet users in the Web-based user administration and B2C self-registration.

Session Security Protection

➡ Recommendation

To prevent access in javascript or plug-ins to the SAP logon ticket and security session cookie(s), we recommend activating secure session management and using SSL to protect the network communications where these security-relevant cookies are transferred.

Session Security Protection

In the Configuration Tool, edit the following properties for the Web Container service. These properties control security-related aspects of HTTP sessions:

Table 320

Property	Recommended Value
`SessionIdRegenerationEnabled`	True
`SystemCookiesDataProtection`	True
`SystemCookiesHTTPSProtection`	True (false if SecuritySessionIDHTTPSProtection is activated)
`SecuritySessionIDHTTPSProtection`	True (false if SystemCookiesHTTPSProtection is activated)

For more information and detailed instructions, see *Session Security Protection* in the *SAP NetWeaver Application Java Security Guide*.

ℹ Note

For Web Channel applications specific configurations have to be made to support the AS Java security settings. This especially the case for Web Channel applications that require the usage of HTTP before a user authentication, and a switch to HTTPS after user authentication. In this case it is `SystemCookiesHTTPSProtection` must be set to *False* and `SecuritySessionIDHTTPSProtection` to *True*.

For more information about configuration of Web Channel applications with regard to the AS Java security settings, see SAP Note 1503236.

Furthermore the Web Channel applications E-Commerce B2B/B2C and E-Service B2B/B2C provide a special XCM configuration to enable the session ID regeneration. For more information, see SAP Note1492234.

The Web Channel applications include a Cross Site Request Forgery (XSRF) protection. The protection is activated by default. It can be deactivated by setting the context parameter *enableXSRFProtection* of the Web descriptor (web.xml) of a Web channel application to *False*. To enable the XSRF protection, you need at least the Patch 18 of Support Package 19 of the Netweaver AS Java release 7.00. For more information, see SAP Note 1501646.

Network and Communication Security

Communication Channel Security

The following communication channels and protocols are used between different components in a Web channel scenario.

Channel and Technology

Table 321

Component A	Component B	Channel	Technology
Web browser	HTTP server (reverse proxy)	Front end to server Communication with Web browser	HTTP/HTTPS (secure)
HTTP server	AS Java/Web channel application	Server to server Requests from Web browser are forwarded to Web channel application running on AS Java. Responses from Web channel are forwarded to the Web browser.	HTTP/HTTPS (secure)
AS Java/Web channel application	CRM or ERP system	Application to server Java-based Web channel application executes application logic running on the SAP system.	RFC/SNC (secure)
AS Java/Web channel application	Internet Pricing and Configurator (IPC)	Application to server Communication for product configuration or pricing	RFC/SNC (secure)
AS Java/Web channel application (SAP CRM)	TREX	Application to server Communication for retrieving catalog data	RFC/SNC (secure)
AS Java/Web channel application (SAP ERP)	TREX	Application to server Communication for retrieving catalog data	HTTP/HTTPS
SAP CRM or SAP ERP	TREX	Server to server for catalog replication	RFC

RFC connections can be protected using Secure NetWork Communication (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

Recommendation

We recommend using secure protocols, such as SSL, or SNC wherever possible.

As shown in the table, you may choose between a nonsecure or secure protocol. The next section gives you the information to decide which protocol meets your security requirements. For more information, see *Transport Layer Security* in the SAP NetWeaver Security Guide.

Guidelines for Selecting Secure Communication Channels

Secure Sockets Layer (SSL)

The SSL encryption protects the data from potential eavesdroppers, providing a higher degree of privacy for the communications (for example, logon or credit card data to the Web shop). The data is also protected from manipulation – any changes made to the data during transfer are detected.

For information about SSL and how to set up SSL on the application server (AS), see the *SAP NetWeaver Security Guide*.

You have to configure the HTTP and HTTPS ports in XCM if you intend to use SSL in your Web channel application, under ▶ *XCM* › *General Application Settings* › *Customer* › *<application name, such as b2b>* › *<appname>config* ◀.

Component Configuration details: **`http.port.core and https.port.core`**

As of SAP CRM 5.2, the variable `$AUTO` is inserted by default. This variable automatically calculates the HTTPS port during runtime. For more information, see SAP Note 1049116.

Communication Channel between WebClient and HTTP Proxy or SAP NetWeaver AS Java

We recommend that you use SSL to protect the traffic between the Web browser and the HTTP server or the SAP NetWeaver AS.

SSL is activated in the various Web channel applications (such as B2B and B2C) after installation.

- In business-to-consumer (B2C), the application switches to SSL when entering the checkout or logon process.
- In business-to-business (B2B) or another application with a logon screen at the beginning, the application automatically switches to SSL when entering the logon screen.

You define whether SSL is used by making configuration settings in the XCM Administration tool: ▶ *General Application Settings* › *Customer* › *<Web application name, such as b2b>* › *SSL-enabled* ◀.

For security reasons, the *SSLSwitchEnabled* flag has to be set to false (this is visible only in B2C).

> **Note**
>
> Web Channel applications must use HTTPS for J2EE security settings. For more information, see SAP Note 1503236

HTTP-Based Communication Channel Between SAP NetWeaver AS Java and TREX

If you want to secure the HTTP-based communication channel to the TREX server, see SAP Note 819143.

Secure Network Communication

Secure network communication (SNC) is used to secure the data communication paths between the various SAP system components.

You can apply the following levels of security protection:

- Authentication only: SNC verifies the identity of the communication partners
- Integrity protection: SNC detects any changes of the transferred data
- Privacy protection: Transferred messages are encrypted

The main focus of SNC usage in Web channel is privacy protection. This is the maximum level provided by SNC.

To set up SNC in Web Channel Enablement, you have to perform the following steps:

- Set up SNC on SAP NetWeaver AS Java and the back-end system (for example, SAP CRM or SAP ERP). Perform various installation steps such as installing an external security product and creating a personal security environment (PSE). For more information, see the *SAP NetWeaver Security Guide*.

- You have to configure SNC-based connection data in every Web application of your Web channel scenario (for example, B2B, B2C, shop administration).

  This is done in XCM using the *ICO* configuration component. Select either the *Secure server connect* or the *Secure group connect* base configuration while creating the connection configuration.

Network Security

Recommendation

We recommend running the SAP Web Channel applications in a secured Network Zone. The figure below introduces a possible Network topology, which is secured by different firewalls and uses a reverse proxy server/ Web dispatcher.

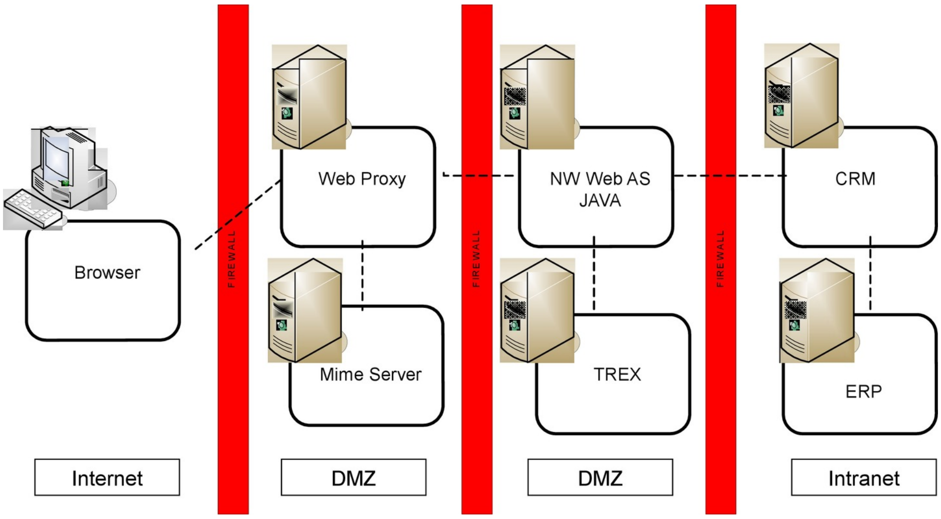


Figure 26: Overview of Possible Network Topology

Note

Currently the business data of SAP NW AS ABAP servers for SAP CRM or SAP ERP can only be accessed synchronously via RFC. It is not possible to replicate required business data between an SAP CRM or SAP ERP back-end server to an SAP NW AS ABAP frontend server.

The SAP Web Channel applications leverage the standard SAP NW AS Java HTTP and HTTPS ports.

For more information, see the following references:

- Services and ports used by SAP NetWeaver

  SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Network and Communication Security* > *Network Services*

- Setting up the Netweaver Application Server Java

  SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the Application Server* > *Security Guides for the AS Java* > *SAP NetWeaver Application Server Java Security Guide* > *Technical System Landscape* and *Network Security* .

- Setting up a firewall

SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Network and Communication Security* › *Using Firewall Systems for Access Control* ›

- Setting up SAP Web Dispatcher

  SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ›: Search for *Administration of the SAP Web Dispatcher*.

- Setting up a reverse proxy

  SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ›: Search for *Configuring Proxy Settings*.

- Setting up SAProuter

  SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ›: Search for *SAProuter*.

- Setting up multiple network zones

  SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Network and Communication Security* › *Using Multiple Network Zones* ›

Ports

The Web Channel applications run on SAP NetWeaver and use the ports from the AS Java.

For more information, see the topics for AS Java Ports in the corresponding SAP NetWeaver security guides. For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see *TCP/IP Ports Used by SAP Applications*, available on the SAP Developer Network at sdn.sap.com/irj/sdn/security ▶ *Infrastructure Security* › *Network and Communications Security* ›. If SSL is used, the corresponding ports can be specified in the *General Application Settings* of a Web application in the *Extended Configuration Management*. The parameters are:

- http.port.core
- https.port.core

Communication Destinations

Connection Destinations from Web Channel Applications

Table 322

Destination	Delivered?	Type	User, Authorizations	Description
Connection to SAP CRM/SAP system	No	RFC	For more information, see the *Authorizations* section above.	Technical user used for stateless or anonymous communication with the back-end system. Configured using application configuration after installation.
Connection to IPC server	No	RFC	No	Configured using the XCM tool after installation.
Connection to TREX	No	RFC	No	The TREX can be configured using manual configuration or dynamic configuration in the XCM. When using dynamic configuration, the values of the RFC

Destination	Delivered?	Type	User, Authorizations	Description
				destination to the Index Management Service (IMS) server are retrieved automatically from the underlying back-end CRM system (provided the value of the parameter *useDynConnParams* is "true"). On choosing this setting, you do not have to specify any other parameter for this component. The other option is manual configuration where you have to manually specify the RFC destination information in the XCM tool (if the value of the parameter *useDynConnParams* is "false"). When you choose this setting, you have to specify the correct RFC connection parameters (gwhost, gwserv, tphost, and tpname) to the IMS server. You can use this manual configuration when different IMS servers (on different machines) serve the same indexes. As a result, different Web applications on one server or different servers are able to access different IMS servers, implementing load balancing or high availability. The distribution and update management of the indexes between such different IMS servers must be performed by other mechanisms. Web Channel Enablement does not provide support for this. At present, security level is not set for both the configurations. After the implementation, the RFC connection between the TREX and the CRM system is secured using SNC. You can also use other methods, such as VPN.
Connection to TREX	No	HTTP	No	For more information about SAP E-Commerce for SAP ERP, see SAP Solution Manager.

⚠ Caution

Do not use the SAP_ALL role for any Internet or technical/service users, but use the roles provided or copies of them.

Data Storage Security

Web channel application data is stored at different storages depending on the data type.

LDAP

If the User Management Engine (UME) is used for authentication in a Web channel application, UME user data can be stored in an LDAP.

Cookies

Cookies store a small amount of data on the client browser. Web Channel Enablement uses the following types of cookies:

- Session cookies

  These cookies are required to keep a client session and are deleted when the browser is closed.

  > ➜ Recommendation
  >
  > Keep session cookies turned on for both security and functional purposes.

- Persistent cookies

  These cookies are used to store data on the client machine.

  > ℹ Note
  >
  > Data storage security may not work if these cookies are disabled. For information about how to control cookie handling, see your Web browser documentation.

The cookie and its data are stored in the Web browser’s file system on the client PC. In B2C and B2B, cookies are used as follows:

- Business-to-consumer (B2C)

  The cookie stores the business partner globally unique identifier (GUID) if a user logs on or registers and maintains a profile. As a result, in Web Channel Enablement, the personalized product recommendation is stored in the cookie if the user maintains the personal data.

- Business-to-business (B2B)

  The order number and order date are stored in the cookie. A new cookie is generated or the existing cookie is updated, when the user creates or changes an order respectively.

Database

In the main business data is stored in the database of the SAP back-end system. For special functionality other data storages are used.

Some data is stored in the database of the SAP NetWeaver AS Java, such as:

- Order templates and shopping baskets

When using the Java basket in the B2B or B2C application, the data is stored in the SAP NetWeaver AS database. All data regarding order templates and shopping baskets is stored in the database without payment information such as the credit card number.

XCM Application Configuration Data

The Web channel application is configured using the XCM administration tool. The customer settings are stored in the local database of the SAP NetWeaver AS Java. Some data is encrypted using the secure storage service of the AS Java before it is stored in the database. The password of the service user is an example of encrypted data.

Note

Sensitive XCM data is only encrypted securely if you have installed the cryptographic toolkit software for Java provided by SAP. We recommend that you install the cryptographic software. If you have not installed the cryptographic software provided by SAP, the data is encoded using base-64 encoding.

For more information about installing the cryptographic software provided by SAP, see SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ◀: Search for *Using the Cryptography Tool*.

If you intend to transport or copy XCM configuration data from one AS Java to another AS Java, you have to copy the keys used to encrypt sensitive XCM data from one server to the other server. This is done in the key storage service of the AS Java. The following procedure describes how you can copy a secure storage key:

1. Log on to the AS Java where XCM data has been encrypted.
2. Select the key storage service.
3. Create a new view, such as `xcmkeycopy`. Since you can only export complete views, a temporary view for exporting the keys is created.
4. Select the keys for the Web applications for which you want to transport the XCM data. Use the *Import from Other* button and the necessary keys from the secure storage view are exported into the newly created view. Every Web application has its own key.
5. Save the `xcmkeycopy` view to file.
6. Log on to the AS Java to which you want to import the keys and select the key storage service.
7. Import the previously exported keys into the secure storage view.

Encryption of Payment Cards

In the SAP Web Channel applications you can use payment cards. For data protection reasons, we recommend that you store the payment card number in an encrypted form on the database.

For information about enabling the encryption of payment card numbers, see section Payment Card Security According to PCI-DSS [page 42].

Caution

Do not assign decryption authorization (`B_CARD_SEC`) to any unauthorized user. Especially roles used for any user within SAP Web channel applications must not be assigned the `B_CARD_SEC` authorization.

Other Security-Relevant Information

Distributed Denial-of-Service (DDOS) Attacks

SAP does not provide in-house DDOS defense tools or mechanisms. Therefore, to address this issue, we strongly recommend that the Web Channel administrator use third-party tools that protect against these types of attacks.

One Step Business Scenario

The callback URL (Hook URL) of the One Step Business Scenario can be secured against URL manipulations. To do this, you have to enter the accepted callback URL in the security configuration of the application configuration of the B2B application using the XCM tool. For more information, see SAP Note 1487217.

JavaScript

The Web channel applications use JavaScript extensively. If JavaScript is disabled on the browser, the application may not work as expected.

Restricting Access to Technical Administration of Web Channel Applications

Every Web channel application has some pages used for technical administration of the Web application.

In addition, the administration area provides the following features:

- Application configuration such as connection parameters to SAP CRM or SAP ERP using the XCM administration tool
- Overview of various caches

For more information about the different features of the administration area, see the configuration information in SAP Solution Manager for the corresponding Web application, such as B2B for SAP ERP or SAP CRM.

For information about XCM, see the Web Channel Enablement installation guides on SAP Service Marketplace at service.sap.com/crm-inst.

You can access the administration pages at `http://<host>:<port>/<appname>/admin`. For example: localhost:50000/b2b/admin .

Note

It is mandatory to restrict access to the application administration pages from the Internet. This should be done by HTTP proxy or a reverse proxy. If you do not have such a proxy you have to turn off the administration pages completely.

Before you expose the application to the Internet, you must secure the application by using stringent security measures as explained in the following sections.

A going-live checklist is available. For more information, see the *Checklist* section below.

Restricting Access to Web Channel Administration Pages from the Intranet

The administration pages are secured using basic authentication. This ensures that users have to provide a username and password before they can access the application.

Note

As of SAP NetWeaver 7.11 Application Server (Java), the administration pages are secured using form authentication by default.

Only users with the isaadmin role have access to the administration pages. After the installation of the application, the administrators group on the AS Java is automatically assigned to this role. The user *Administrator* is always a part of the administrators group.

Recommendation

Do not use the *Administrator* user for administering the Web application. The administrator of the Web application should have fewer rights than the administrator of the AS Java. For example, the Web application administrator should not be able to shut down the AS Java.

Instead of using the AS Java administrator, a new user should be created, such as **`ecommerceadmin`**, and assigned to the isaadmin role.

The following steps describe how to create a new user on AS Java:

1. Log on to the J2EE Engine using the Visual Administrator.
2. Select the *Security Provider* service of the J2EE Server.
3. Choose the *User Management* tab.
4. Choose *Create User*.
5. Enter the name of the user, for example, isaadmin.
6. Enter the password for the user.
7. Choose *OK*.
8. Choose the *Policy Configurations* tab.
9. Select the Web channel for which you are the administrator, for example, `sap.com/crm.b2b*b2b`.
10. Choose the *Security Roles* tab.
11. Select the isaadmin role.
12. Assign the previously created user to the role.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *J2EE Engine Configuration*.

Restricting Access to Web Channel Administration Pages from the Internet

> **Note**
>
> Define as few mappings as possible. The HTTP server should allow requests that are required by your application. All other requests must be blocked.

To prevent access to the Web channel administration, use one of the following methods, and follow the steps or examples given:

- Using Microsoft Internet Information Server (IIS) HTTP server in front of AS Java

  You have an HTTP server between the AS Java and the Internet. You can restrict the access through the Web server for the following pages:

  `/<applicationname>/admin.`

  You can restrict access by using the IisProxy, for example:

  Syntax

```
<ISAPI-config version=”1.6”>
<filter name=”IisProxy filter” />
<extension name=”IisProxy extension” />
<mapping name=”B2B Secure Admin Area”>
<source>
<protocol>http</protocol>
<prefix>/b2b/admin/prefix>/b2b/admin/>
<new-prefix>/error/</new-prefix>
</source>
<target>
<protocol>http</protocol>
<host>localhost.your.corp</host>
<port>51000</port>
</target>
</mapping>
```

```
<mapping name=”B2B Application”>
<source>
<protocol>http</protocol>
<prefix>/b2b/</prefix>
</source>
<target>
<protocol>http</protocol>
<host>localhost.your.corp</host>
<port>51000</port>
</target>
<compress-types>text/html, text/plain</compress-types>
</mapping>
</ISAPI-config>
```

The mapping to the Web channel administration leads to a nonexistent area or an error.

- Using Apache HTTP server in front of AS Java

  For more information about security-relevant settings of the Apache HTTP server, see:

  - Apache HTTP Server Version 1.3:

    httpd.apache.org/docs/misc/security_tips.html

  - Apache HTTP Server Version 2.0:

    httpd.apache.org/docs-2.0/misc/security_tips.html

  - Configuration example:

    ```
    # Enable Access Control and Reverse Proxy
    AddModule mod_access.c
    AddModule mod_proxy.c
    # Deny Access to ADMIN pages
    <Directory proxy:*/admin/*>
    Order Deny,Allow
    Deny from all
    </Directory>
    # Deny Access to WEB-INF Directories
    <Directory proxy:*/WEB-INF/*>
    Order Deny,Allow
    Deny from all
    </Directory>
    # Configure Reverse Proxy for SAP J2EE
    ProxyRequests Off
    ProxyPass /b2c http://<j2ee_server>:50000/b2c
    ```

- No HTTP server in front of AS Java

  You must turn off all the features of administration. For more information, see the *Turning Off Features of Administration Area* section below.

  Check whether the mappings are correct by performing a security check as described in the checklist.

Turning Off Features of Administration Area

You can turn on or off access to each feature of the administration area by using the following context parameter in the web.xml: adminconfig.core.isa.sap.com.

> **Note**
>
> If you have restricted access to the administration pages using HTTP mappings as described in the previous section, you do not need to use this feature. However, if you access the application directly from the Internet using the HTTP server within the AS Java, we recommend that you follow the instructions in this section.

The value of this parameter contains a list of keywords separated by commas. Each keyword is associated with a feature in the administration area. Therefore, when you remove a keyword, the corresponding feature is disabled.

The settings can be changed using the J2EE Engine Visual Administrator in the Web container service as follows:

1. Log on to the J2EE Engine using the Visual Administrator.
2. Select the *Web Container* service of the J2EE Server.
3. Select the required Web application.
4. Choose *View*.

   A new panel opens.
5. Choose the *Context Parameters* tab.
6. Select the adminconfig.core.isa.sap.com context parameter.
7. Change the setting.
8. Choose *Modify*.

   > **Note**
   >
   > After changing the settings, you must restart the Web application. We recommend that you disable all administrative features by removing the value from the adminconfig.core.isa.sap.com context parameter.

The following table provides an overview of the available features:

Table 323

Feature	Description	Access After Installation (not all Web applications support all settings in this table)
Isacorecache	Application core caches	Yes
Catalogcache	Web catalog cache	Yes
Corecache	System-level cache	Yes
Jcoinfo	Information about SAP Java Connector	Yes
Logging	This feature is not supported as of SAP CRM 5.2 and is kept for downward compatibility. Logging is configured centrally in the J2EE Engine. For information about Web Channel Enablement logging, see SAP Solution Manager. For information about how to configure logging, see the documentation for the Visual Administrator. For more information about logging with SAP E-Commerce, see SAP Note 1090753.	Yes

Feature	Description	Access After Installation (not all Web applications support all settings in this table)
Version	This feature is not supported as of SAP CRM 5.2 and is kept for downward compatibility. For information about how to obtain version information for the Web channel application, see the *SAP Customer Relationship Management Operation Guide* on SAP Service Marketplace at service.sap.com/instguides.	Yes
Xcmadmin	Turns access to XCM administration tool on or off	Yes
Ccmsheartbeat	For more information about Web channel supportability, see *SAP Customer Relationship Management Operation Guide* on SAP Service Marketplace at service.sap.com/instguides.	Yes
Dbmig	Controls whether the migration tool for SAP CRM 4.0 shop data in the SAP CRM 5.2 (or higher) database is turned on.	Yes
Scheduler	Controls whether schedule administration is accessible.	Yes

The following administration features are controlled by XCM:

Table 324

Feature	Description	Access After Installation
Appinfo	You can control this feature using the XCM administration tool under *General Settings* › *Customer* › *<application name, for example, b2b>* › *<application name>config* › *appinfo* This feature must be turned off in production.	No
show.start.jsp	A list of available XCM configurations is displayed if you start the application as follows: **`http://<host>:<port>/<application name, for example, b2b>/`** You can control this feature using the XCM administration tool under: *General Settings* › *Customer* › *<application name, for example, b2b>* › *<application name>config* › *showStartpage* This feature must be turned off in production.	No
Sat	Specifies whether single activity trace is turned on. For more information, see SAP Solution Manager.	No

Disabling XCM Application Configurations

XCM enables you to create multiple configurations of your Web channel application. You can even run different applications using different configurations at the same time.

> **Note**
>
> You have to make sure that you turn off or delete all the application configurations that are not used in the production environment.

To disable application configurations, do the following:

1. Start XCM of the Web application.
2. Choose *Edit*.
3. Choose the tree and select ▶ *Start* › *Application Configuration* › *Customer* ◀ <the configuration you do not want to use>.
4. Deselect the *Active Configuration* checkbox.
5. Choose *Save Configuration*.
6. Perform steps 3 to 5 for every configuration that is not used in production environment.
7. To release the lock on XCM configuration, choose *Display*.

For more information about the usage of the XCM tool, see SAP Solution Manager.

Encryption of Payment Cards

In the Web channel business-to-business (B2B) and business-to-consumer (B2C) applications, you may use payment cards. For data protection reasons, we recommend that you store the payment card number encrypted on the database. For information about how to enable the encryption of payment card numbers, see section Payment Card Security According to PCI-DSS [page 42].

Disabling Call Center Agent Mode

The call center mode enables a call center agent to act on a customer's behalf. For example, agents may need to check the customer's baskets, orders, or personal data and even create orders.

To disable the call center agent mode, in XCM administration, select the following checkbox:

▶ *Components* › *Customer* › *user* › *CallCenterMode: false* ◀

> ➔ Recommendation
>
> Disable the call center agent mode. In this mode, it is possible to logon using single-sign on (SSO). No logon screen appears if an SSO ticket exists and the user enters the B2C shop.

Trace and Log Files

In contrast to previous versions of Web Channel Enablement, logging and tracing is now configured centrally using the log configuration service of the AS Java. The service is configured using the Visual Administrator tool of the AS Java.

Make sure that the severity level for the following locations is set to ERROR:

- com.sap.isa
- com.sap.eservice

Session Trace

Web channel supports a single-session trace. This trace is used to obtain the information for a particular session. This function is used by developers or by support in customer projects. To switch on the trace, perform the following steps:

- Open the start page of the Web application

  ```
  http://<server>:<port>/<application name, for example, b2b>
  ```

  The page has to be turned on (▶ *XCM Start* › *Customer* › *<Web application name, for example, b2b>* › *showStartpage (true)* ◀)
- Click the *Single Session Trace* for the application configuration that you want to trace.

All trace information related to the session is written into the default trace of the SAP NetWeaver AS Java and can be viewed with the Log Viewer.

> **Note**
>
> The trace also traces the whole HTTP-based communication, such as passwords and credit card numbers, between the Web client and AS Java. If you want to make sure that no one else can see this information, you have to delete the default traces of the SAP NetWeaver AS Java (`\usr\sap\<SID>\<Instance name>\j2ee\cluster\server0\log\defaultTrace`).

Checklist

The following check list is a mandatory going-live checklist. Ensure that your application adheres to all the requirements specified in this checklist:

Protecting Web Channel Administration Pages and Functions

Table 325

Security Item	Method	Reference	Result/ Comments
Check whether access to the Web channel administration area is restricted from the intranet. Log on using the user created during Web channel installation.	Call the administration area from the intranet, for example: **`http://<host>:<port>/b2b/admin`**.	N/A	A logon window must appear. Log on using the user created during Web channel installation.
If your application is exposed to the Internet, make sure that access to the administration is restricted from the Internet.	Call the administration area from the Internet, for example: **`http://<host>:<port>/b2b/admin`**.	See the *Restricting Access to Technical Administration of Web Channel Applications* subsection above.	A logon window must not appear. The HTTP proxy must not forward the request to the administration area.
Check whether the administrator password is blank.	Call the administration area from the intranet, for example: **`http://<host>:<port>/b2b/admin`**. User – Administrator Password – leave blank	N/A	You must not be able to log on.
Check whether appinfo feature is turned off. This feature must be turned on only during development.	Call the application with additional appinfo request parameter, for example: **`http://<host>:<port>/b2b/b2b/.init.do?appinfo=true.`**	See the *Turning Off Features of Administration Area* subsection above.	You must not be prompted to log on. A second browser window that provides system information must not be opened.
Ensure that the showstacktrace switch is turned off.	Check in XCM – component UI value `showstacktrace. isacore` should be assigned to the application configuration you are using.	N/A	The value must be false (off).

Security Item	Method	Reference	Result/ Comments
Ensure that the showjspdebugmsg switch is turned off.	Check in XCM – component UI value `showjspdebugmsg.core` should be assigned to the application configuration you are using.	N/A	The value must be false (this switch is not available in all Web channel applications).
Disable or delete all XCM configurations that are not needed	Disable or delete all XCM configurations that are not used in production.	See the *Disabling XCM Application Configurations* subsection above.	All disabled configurations are marked in red in the XCM tree.
Make sure that HTTP-based file browsing is turned off.	Call the application using **`http://<host>:<port>/b2b/b2b`**.	See SAP Note 531495	You must not see any directory content.

Protecting XCM Scenarios Using “catalogstatus = inactive”

Make sure XCM scenarios where `catalogstatus` is set to `inactive` for component `webcatalog` are not accessible from the Internet.

For more information, see SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Master Data* › *Product Catalog* › *Product Catalog Staging*.

Protecting Internet Pricing and Configurator (IPC) Price Analysis Tool

Table 326

Security Item	Method	Result/Comments
Ensure that IPC price analysis and enable pricing conditions display is turned off.	Check in XCM – component UI value `enable.priceAnalysis`	The value must be false.

Protecting Web Channel Administration Pages or Functions

Table 327

Security Item	Reference
Voice over IP (VoIP) in Web collaboration uses the NetMeeting Active X control.	See SAP Note 725954

6.1 E-Service

Why Is Security Necessary?

Security is important because any business-related information can be accessed and your application can be the target of many different attack scenarios. The guidelines listed here apply in addition to the guidelines in Component-Specific Guidelines: Web Channel Enablement [page 241].

Technical System Landscape

The following figure shows the components that are required for the SAP Internet customer self-service (ICSS) Java application:

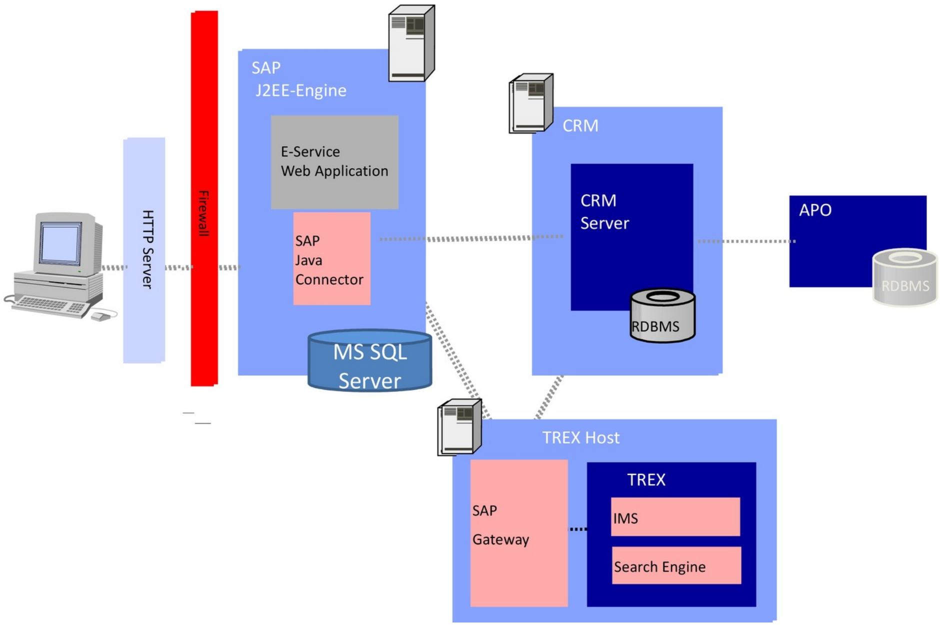


Figure 27: Components required for ICSS

User Administration and Authentication

User Management

The e-service applications run using users that can be maintained by using the *User Maintenance* (SU01) transaction and provide their services to any user connected to a business partner who is a contact person (B2B) or consumer (B2C).

User Management Tools

In section Component-Specific Guidelines: Web Channel Enablement [page 241], see the subsection *User Management Tools for All Web Channel Scenarios*.

The SU05 user concept is not supported by e-service applications.

User Types

In section Component-Specific Guidelines: Web Channel Enablement [page 241], see the subsection *User Types*.

User Data Synchronization

For E-Service B2B Internet Users, the Web-based User Management can be used. For more information, see the sections *Support of the User Management Engine (UME)* and the *User Data Synchronization* in the Component-Specific Guidelines: Web Channel Enablement [page 241].

Authorizations

The following table lists the PFCG user roles that are provided for ICSS B2B and B2C to provide minimum authorizations to users and prevent unauthorized access to the application or for a part of the application.

> Note
>
> The anonymous user is used in business-to-consumer (B2C) scenarios to provide access to functions not requiring password protection, such as FAQ and solution search. This kind of user is not authorized to access other sensitive functions and therefore we recommend that you restrict its access.

Delivered Roles

Table 328

Delivered Role	Scenario	Description
SAP_CRM_ECO_ISE_WU_B2B	B2B	Internet user role
SAP_CRM_ECO_ISE_TU_B2B	B2B	Service user role
SAP_CRM_ECO_ISE_WU_B2C	B2C	Internet user role
SAP_CRM_ECO_ISE_TU_B2C	B2C	Service user role

The following table lists the PFCG user roles that are provided for complaints and returns, entitlement inquiries, and remanufacture inspections to provide minimum authorizations to users and prevent unauthorized access to the application or a part of the application.

Delivered Roles

Table 329

Delivered Role	Scenario	Description
SAP_CRM_ECO_ISE_WU_CR	B2B	Internet user role
SAP_CRM_ECO_ISE_TU_CR	B2B	Service user role
SAP_CRM_ECO_ISE_WU_INSP	B2B	Internet user role
SAP_CRM_ECO_ISE_TU_INSP	B2B	Service user role
SAP_CRM_ECO_ISE_WU_ENT	B2B	Internet user role
SAP_CRM_ECO_ISE_WU_ENT_VIEW	B2B	Internet user role
SAP_CRM_ECO_ISE_TU_ENT	B2B	Service user role

Data Storage Security

The application data is stored in SAP CRM.

> **Note**
>
> No persistent cookies are used. No data is stored on the client side. For more information, see *XCM Application Configuration Data* under Component-Specific Guidelines: Web Channel Enablement [page 241].

6.2 Interactive Product Configuration User Interface

This section provides information about the security aspects of the product configuration Web application running the sales and service scenarios in SAP Customer Relationship Management (SAP CRM).

The security-relevant topics of the basis components, such as SAP NetWeaver Application Server Java (SAP NetWeaver AS Java), are described in detail in the corresponding security guides. For more information, see Component-Specific Guidelines: Web Channel Enablement [page 241].

Related Security Guides

Table 330

Application	Guide	Most-Relevant Sections or Specific Restrictions
CRM Web channel (Web channel) enablement	Web channel enablement	- *Data Storage Security* For Extended Configuration Management (XCM) customer configuration data - *Other Security-Relevant Information* For Internet sales administrator area - *Trace and Log Files*
SAP NetWeaver	*Security Guide for SAP NetWeaver* on SAP Help Portal at help.sap.com/nw_platform	- *How to Configure Secure Sockets Layer (SSL)* - *How to Install Secure Network Communication (SNC)*

Why Is Security Necessary?

The browser communicates with the product configuration Web application on SAP NetWeaver Application Server Java (SAP NetWeaver AS Java) using HTTP or HTTPS. Whether you need to use HTTPS depends on the type of data displayed within the interactive product configuration UI, which in turn depends on your configuration model. If the user needs to enter sensitive data, you should use HTTPS.

The product configuration Web application communicates over the network with the CRM system using remote function call (RFC). The communication must be secured to prevent someone from eavesdropping on this communication to get data such as account credentials, passwords, or content.

The product configuration Web application also provides features for the convenience of the user that could be regarded as not secure in some scenarios. For example, import or export of configurations can reveal unwanted information to the user or give users the option of manipulating exported configurations and reimporting them. Although this might be acceptable in an in-house scenario, it is unwanted in an Internet scenario.

All security-relevant features can be turned off with one switch in the XCM configuration: *IPC Security Level*. The following table explains the different security levels and their effects on the product configuration Web application:

Product Configuration Security Levels

Table 331

Security Level	Description
0	All features of the Web applications are enabled
1	Secure mode (default) Features considered as not secure are disabled Import/export of configuration data to the local client is disabled

IPC Security Level is an XCM parameter that can be maintained using the XCM administration tool. For information about setting XCM parameters, see ▶ *IPC Configuration Support* › *Extended Configuration Management* ◀.

Important SAP Notes

Table 332

SAP Note Number	Short Text	Comment
412309	Authorization profile RFC user for IPC	Only scenario C relevant
896242	Role for IPC JCO user	Information about the role that must be used for the IPC JCO user.

User Administration and Authentication

User Types

The SAP CRM back-end user is used by the product configuration Web application to connect to the CRM back-end system. It must have the role `SAP_IPC` to have the required authorizations. In the XCM administration tool, the credentials of this back end user have to be maintained. For more information, see SAP Solution Manager. For information about authorizations, see the *Authorizations* subsection below.

User Management

Table 333

Tool	Description
SAP NetWeaver Application Server Java (SAP NetWeaver AS Java) user management using the SAP NetWeaver Administrator	Access to administration pages that are part of every Web channel application, is controlled using SAP NetWeaver AS Java security.
User and role maintenance with SAP NetWeaver AS ABAP (Transactions SU01, PFCG)	For more information, see the documentation for the *User Maintenance* transaction.

User Types

Table 334

System	User	Delivered?	Type	Default Password	Description
SAP NetWeaver AS Java	Administrator	Yes (part of SAP NetWeaver AS Java installation)	User administered on SAP NetWeaver AS Java	As defined during installation of SAP NetWeaver AS Java	This user can be used to enter the Web channel applications administration pages. For more information, see Extended Configuration Management (XCM) in SAP Solution Manager. We recommend that you create a new user with fewer rights for administration of Web channel applications instead of using the SAP NetWeaver AS Java administrator (see next row).
SAP NetWeaver AS Java	Isaadmin	No	User administered on SAP	No	We recommend that you create this user after installing SAP NetWeaver AS

System	User	Delivered?	Type	Default Password	Description
			NetWeaver AS Java		Java (together with the SAP CRM Java applications). For more information, see below *Restricting Access to Web Channel Administration Pages* from the Internet, under *Other Security-Relevant Information*.
SAP CRM	Service (anonymous) user	No, but role SAP_IPC is delivered (see SAP Note 896242)	Service user created using the User Maintenance (SU01) transaction	No	User for establishing the connection between SAP CRM and the product configuration Web application. For more information, see the Authorizations section below. The user must be entered in the XCM IPC configuration. For Authorization assignment, see next section, Authorizations.
SAP CRM	Internet User	No, but role SAP_IPC is delivered (see SAP Note 896242)	Dialog User created using the User Maintenance (SU01) transaction	No	User that uses product configuration

User Data Synchronization

The synchronization of user data is not applicable.

Logon Processes

As of SAP CRM 7.0, the product configuration Web application uses the logon module provided by the Web channel environment and consequently accepts SAP Logon tickets (transaction SS02) as the logon procedure. For more information, see Component-Specific Guidelines: Web Channel Enablement [page 241].

Integration with Single Sign-On Environments

The product configuration Web application uses the central logon module of the Web channel environment, therefore it accepts SAP logon tickets (transaction `SSO2`) as the logon procedure. For more information, see Component-Specific Guidelines: Web Channel Enablement [page 241].

Authorizations

For authorization information common to all Web channel applications, see the *Authorizations* section under Component-Specific Guidelines: Web Channel Enablement [page 241].

User Roles

Service and Individual users that use product configuration need certain standard product configuration roles. These roles are listed in the following table:

Table 335

Role	Description
SAP_IPC	Authorization to use the product configuration Web application. See SAP Note 896242

Network and Communication Security

Communication Channel Security

The following communication channels and protocols are used between different components:

Table 336

Component A	Component B	Channel	Technology
Web browser	HTTP server (reverse proxy)	Front-end to server Communication with Web browser	HTTP/HTTPS (secure)
HTTP server	AS Java/ product configuration Web application	Server to server Requests from Web browser are forwarded to the product configuration Web application running on AS Java. Responses from product configuration are forwarded to the Web browser.	HTTP/HTTPS (secure)
AS Java/ product configuration Web application	SAP CRM	Application to server Java-based product configuration Web application executes application logic running on the SAP system	RFC/ SNC (secure)

In most cases, you can choose between nonsecure and secure protocols. For information to help you decide which protocol (SSL or SNC) meets your security requirements, see *Secure Socket Layer (SSL)* and *Secure Network Communication (SNC)* under the *Guidelines for Selecting Secure Communication Channels* section in Component-Specific Guidelines: Web Channel Enablement [page 241].

Network Security

For information about network security, see *Network Security* under Component-Specific Guidelines: Web Channel Enablement [page 241].

Communication Destinations

Table 337

Destination	Delivered?	Type	User, Authorizations	Description
Connection to SAP CRM/SAP system	No	RFC	For more information, see the *Authorizations* subsection.	Technical user used for communication with the back-end system. Configured using XCM tool after installation.

Data Storage Security

No data is stored in the product configuration Web application. The results of configuration and pricing are stored in the applications that call product configuration, such as the CRM order.

The product configuration Web application stores administration data only. For more information, see *XCM Application Configuration Data* under Component-Specific Guidelines: Web Channel Enablement [page 241].

A Web browser is required as the user interface. Session cookies, which are deleted when the Web browser is closed, are used to handle the client session. The cookie does not store any other data. On the client side, no user data is stored. For more information, see ▶ *Data Storage Security* › *Cookies* ◀ under Component-Specific Guidelines: Web Channel Enablement [page 241].

Security for Additional Applications

Security is necessary for other components using the product configuration Web application. For information about how to secure these components, see the corresponding security guides.

Other Security-Relevant Information

The product configuration Web application uses JavaScript extensively. If JavaScript is disabled on the browser, the application does not work. In addition, the application uses session cookies, which are deleted when the Web browser is closed, to keep a client session. If the cookies are disabled, the application works correctly if the configuration of the AS Java is configured to allow session handling using URL.

> **Note**
>
> No persistent cookies are used.

For information about the Web-based administration tool, see ▶ *Other Security-Relevant Information* › *Restricting Access to Technical Administration of Web Channel Applications* ◀ under Component-Specific Guidelines: Web Channel Enablement [page 241].

Checklist

Table 338

Feature	Check	How to Check
Web channel administration console	Go to the administration area: `http://<host>:<port>/ipc/admin` Go through the checklist under Protecting Internet Sales Administration Pages/Functions in E-Commerce.	All items mentioned in this checklist must be addressed.

Feature	Check	How to Check

Knowledge base selection	Go to the knowledge base selection:
	`http://<host>:<port>/ipc/ipc/init.do?`
	`scenario.xcm=crmproductsimulation`
		A logon dialog box appears. Log on with the user that was created during Web application installation.
		For more information, see the checks for the Web channel administration console.

Product configuration security level	In XCM, check the security level	The value must be `1` (secure mode).

7 Component-Specific Guidelines: Partner Channel Management

User Administration and Authentication

The type of the user administration differs depending on the use of SAP E-Commerce for SAP Customer Relationship Management (SAP CRM) or SAP ERP or the WebClient UI as explained in the following sections.

User Management Tools When Using SAP E-Commerce for SAP CRM Within Portal (Partner Channel Management)

Table 339

Tool	Description	Prerequisites
Web-based user management	For more information, see SAP Solution Manager.	Only applicable for business-to-business (B2B) users created using the *User Maintenance* (`SU01`) transaction. Authentication value `SU01` (user ID) must be used. Only for SAP E-Commerce for SAP CRM.

User Types for SAP E-Commerce for SAP CRM and Partner Channel Management

Table 340

System	User	Delivered?	Type	Default Password	Description
SAP CRM	Service (anonymous) user for stateless connection	No	Service user created using the *User Maintenance* (`SU01`) transaction	No	User for establishing the stateless connection between SAP CRM and SAP E-Commerce.
SAP CRM	SAP E-Commerce user	No	Dialog user created using the *User Maintenance* (`SU01`) transaction	No	The user that logs on to SAP E-Commerce. The full state SAP E-Commerce connection is established with it.
SAP CRM	SAP E-Commerce user	No	User created using the *Maintain Internet User* (`SU05`) transaction	No	The user that logs on to SAP E-Commerce.

User Management Tools When Using WebClient UI (Partner Channel Management)

Table 341

Tool	Description	Prerequisites
Web-based user management	For more information, see SAP Solution Manager.	Only applicable for B2B users created using the *User Maintenance* (`SU01`) transaction. Authentication value `SU01` (user ID) must be used.

User Types for Partner Channel Management

Table 342

System	User	Delivered	Type	Default Password	Description
SAP CRM	End User	No	Dialog User	No	User created using the User Maintenance (`SU01`) transaction

For information on Partner Channel Management user types, see User Management [page 18].

Authorizations

Partner channel management (PCM) users have access to the WebClient UI applications as well as to the SAP E-Commerce (Web channel) applications. To use both type of applications, the PCM users need authorizations for the WebClient UI and CRM Web channel, so SAP delivers the WebClient UI roles and the Web channel roles.

Collective Roles for Partner Channel Management

Table 343

`SAP_CRM_UIU_CHM_CHANNELMAN_COL`	Composite role for channel managers
`SAP_CRM_UIU_CHM_PARTNERMAN_COL`	Composite role for partners in channel management

These collective roles in the standard system contain all the required roles for the channel manager and the partner manager respectively. The roles included in these collective roles should be sufficient and restrictive for the functional access to the users.

Roles Specific to Partner Channel Management

The following table lists the roles specifically delivered for PCM users, so that they have even more restricted capability than the normal WebClient UI and Web channel users:

Table 344

Role	Description
`SAP_CRM_UIU_CHM_CHANNELMANAGER`	CRM PCM UIU role for channel managers
`SAP_CRM_UIU_CHM_PARTNERMANAGER`	CRM PCM UIU role for partner managers
`SAP_CRM_CHM_CORPORATEPARTNER`	CRM PCM role for corporate partner managers (Only relevant for the Marketing Development Funds (MDF) scenario)
`SPA_CRM_CHM_ISA_WU_B2B_FULL`	B2B with full document authorization

Role	Description
SAP_CRM_CHM_ISA_WU_BOB_FULL	Business-on-behalf (BOB) with full sales order document and quotation authorizations
SAP_CRM_CHM_ISA_WU_HOM_FULL	Hosted order management with full authorizations
SAP_CRM_CHM_ISE_WU_B2B	CHM ICSS role for Internet service users (B2B scenario)
SAP_CRM_ECO_CHM_WU_SHRDCAT	CHM Internet user for shared catalog application
SAP_CRM_CHM_ISA_CM_USERADMIN	SAP E-Commerce user management for channel managers
SAP_CRM_ECO_CHM_TU_SHRDCAT	CRM_ECO: Service user for channel management shared catalog application

These roles ensure that the restrictions delivered in the UIU roles (the first two in the list) are not violated due to the extra authorizations granted in the Web channel roles.

The corresponding roles are already assigned to the collective roles.

In case of service users for PCM, one should replace the Web channel TU role with the corresponding *CHM*TU* role, if one is available.

For the complete list of Web channel roles, see the list of roles in the section Component-Specific Guidelines: Web Channel Enablement [page 241].

Partner Channel Management

In PCM, the roles are delivered along with external services transactions in the user menu. The external services transaction is a simple method to assign authority objects and their values to different roles. The list of external services transactions assigned to a role can be viewed in the menu tab of the roles.

External services transactions are defined in *Maintain the Assignment of Authorization Objects* (transaction SU22) (type LS), for each UIU component. SAP delivers them for all partner-related applications. The default values are set up according to the PCM scenario delivered in the standard system.

The Access Control Engine (ACE) is another important step towards authorizations in PCM. The ACE is designed to help control user access, and is used with the ABAP authorization concept to help control user access to the applications and data. This means that you can, in addition to measures taken on other architecture levels, use application logic to define which users see which data, and whether those users have authorization to read, edit or delete that data. For more information, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *Basic Functions* > *CRM Access Control Engine* and the section Access Control Engine [page 324].

Take into account the additional security measures described in the section Security for Third-Party or Additional Products [page 39]. You could also consider alternative landscape topologies including, but not limited to, the set-up of separate SAP CRM instances for PCM scenarios and processes. The chosen topology would, of course, depend on your security policies with regard to access of external parties to your business systems.

The following roles for PCM are in the standard system:

Table 345

Role	Description
SAP_CRM_UIU_CHM_PARTNERMANAGER	Partner Channel Management – Partner Manager

Role	Description
SAP_CRM_UIU_CHM_CHANNELMANAGER	Partner Channel Management – Channel Manager The CRM roles above are also used for SAP E-Commerce in partner channel management.
SAP_CRM_CHM_CORPORATEPARTNER	Partner Channel Management - Corporate Partner Manager This role grants additional ACE rights for the corporate users and the profile generator (PFCG) transaction authorizations that are required for the corporate user.

Your Customizing settings dictate whether or not the standard values are used. In case Customizing is changed, the values for certain authorization objects (which use customized values) should change as well.

If the scenario implementation at the customer's site had new or enhanced features, this might also require enhancements to authorizations.

For information on generating roles, see Authorizations [page 25].

Transaction (Process) Types for Partner Roles Controlled with Authorizations

The standard mechanism of authorization checks is used for allowed transaction types for a given role or user.

The authorization objects for a user are: CRM_ORD_LP and CRM_ORD_PR. For more information about the settings, see the documentation of these objects in the system. The allowed transaction types are set in object CRM_ORD_PR.

Note that the authorization given in the first object overwrites the authorization allowed in the second one.

Now you have to decide whether to adopt the delivered standard authorizations, which would be set up in the PCM roles, or to extend or adapt them to customer-specific transaction types.

If new transaction types are required for channel business, create new roles and extend the authorizations for the above-mentioned objects accordingly.

Loyalty Management for Partner and Channel Manager Roles Controlled with Authorizations

The standard mechanism of authorization checks is used for allowed transactions for a given role or user. The authorization objects for a user with channel and partner manager roles are: CRM_LOY, CRM_LOYAGR, CRM_LOYRES, LOY_BNFT, LOY_BNGR, LOY_MA, LOY_MSH, LOY_PPA, LOY_PSH, and LOY_PT_ACT. For more information about the settings, see the system documentation for these objects.

Restriction of Access by External HTTP and HTTPS Requests

In addition to the existing authorization structure, you can use Business Add-In (BAdI) *BAdI: Restriction of Access to WebClient UI Framework* (WCF_RESTRICT_ACCESS_BADI) to restrict external HTTP and HTTPS requests from accessing the PCM application.

You can use the active BAdI implementation WCF_RESTRICT_ACCESS_BADI_PCM or create a custom-defined BAdI implementation. The BAdI implementation WCF_RESTRICT_ACCESS_BADI_PCM is called when the WebClient UI is launched. To trigger the execution of the BAdI implementation WCF_RESTRICT_ACCESS_BADI_PCM and to ensure that the BAdI implementation is executed for external requests only, you must define in the Web dispatcher that the HTTP header field x-sap-crm-external-client is added to all incoming HTTP and HTTPS requests to the SAP CRM system.

For more information, see the following references:

- Customizing for *Customer Relationship Management* under ▶ *UI Framework* ▸ *UI Framework Definition* ▸ *Business Add-Ins (BAdIs)* ▸ *BAdI: Restriction of Access to WebClient UI* ❯
- Documentation for BAdI interface `IF_WCF_RESTRICT_ACCESS_BADI`
- Documentation for BAdI method *Get List of Allowed Business Roles* (`GET_BUSINESS_ROLE_WHITE_LIST`)
- Documentation for BAdI method *Get List of Allowed WebClient UI Components* (`GET_UI_COMPONENT_WHITE_LIST`)

Data Storage Security

In additional to the standard security concept for data security and privacy in PCM Access Control, the Access Control Engine (ACE) is used. The access to the data for the users is defined through a set of predefined rules in ACE. This set of rules is applied to the data when it is being created and stored, and from this, an access control list (ACL) is generated. This ACL is then used during runtime to determine the extent of access the user has to the data.

The decision to activate or not to activate ACE depends on whether or not document-level access checks are required for the users. The activation decision is now at the following levels:

- System
- Users/User groups
- Object types

To use ACE, you must make the settings in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* ▸ *Access Control Engine* ❯.

In addition, you can define your own rules and access rights to provide additional access control based on your business requirements.

For PCM, the following ACE packages are delivered with preconfigured user groups and rights for different object types:

- `SAP_CRM_CHM_OO` (Channel Management Workpackage for One Order)
- `SAP_CRM_CHM_ACCOUNT` (Channel Management Workpackage for Accounts)
- `SAP_CRM_CHM_PROD` (Channel Management Workpackage for Products)
- `SAP_CRM_MDF_ACCOUNT` (MDF Workpackage for Accounts)
- `SAP_CRM_MDF_MKTG` (MDF Workpackage for Marketing)
- `SAP_CRM_MDF_OO` (MDF Workpackage for One Order)

For activation of these packages, use the *ACE Activation Tool* (`ACE_ACTIVATION`) transaction. For more information, see the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* ▸ *Access Control Engine* ❯.

In case of SAP E-Commerce applications, the access to products is restricted by the catalog. Rights delivered in the product package would grant display access to all the products.

Activation of these packages would ensure ACE security for PCM.

7.1 Channel Sales Management for High Tech

SAP Customer Relationship Management (SAP CRM) enables the channel sales management for high tech scenario by including the following functions that are modeled as different applications:

- Design registration based on SAP Customer Relationship Management (SAP CRM) enterprise opportunities

- Bill-up
- Channel inventory management
- Channel inventory reconciliation
- Inventory reporting
- Resale tracking and claim management
- Price protection
- Sell-in (sales to channel partner)
- Transmission management

These applications enable processing of various data related to channel sales, which includes creation of sales documents in SAP CRM and sales and invoicing documents in the back-end ERP system.

Why Is Security Necessary?

Security is necessary because within the channel sales management for high tech scenario, the system does the following:

- Accesses data in SAP CRM, such as resale information, channel inventory information, price protection information, and other information related to channel sales that is maintained in SAP CRM
- Leads to creation of sales documents in SAP CRM (which are replicated and invoiced in the back-end ERP system)

It is therefore important to restrict access to this data.

User Administration and Authentication

The channel sales management for high tech scenario uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server (SAP NetWeaver AS). 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 the channel sales management for high tech scenario.

In addition to these guidelines, this section includes information about user administration and authentication that specifically applies to the channel sales management for high tech scenario.

This section lists the tools to use for user management, the types of users required, and the standard users that are delivered with the channel sales management for high tech scenario.

User Management

User management for the channel sales management for high tech scenario uses the mechanisms provided by the SAP NetWeaver AS ABAP such as tools, user types, and password policies. For an overview of how these mechanisms apply for the application, see the sections below. In addition, we provide a list of the standard users required for using the channel sales management for high tech scenario.

User Management Tools

Table 346

Tool	Description	Prerequisites
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (SU01) transaction and the profile generator (PFCG) transaction	For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *Function-Oriented View* >	None

Tool	Description	Prerequisites
	Security › *Identity Management* › *User and Role Administration of Application Server ABAP* ›.	

User Types

The following users must be created for the channel sales management for high tech scenario:

Table 347

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access channel sales transactions. Created by an SAP CRM system administrator.
SAP CRM	N/A	No	System user	No	Mandatory user who can process background jobs.
ERP back end	End user	No	Dialog user	No	Mandatory user who can create sales and invoicing documents, which are posted into the sell-in application in the channel sales management for high tech scenario in SAP CRM.
ERP back end	N/A	No	System user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, the user can be an individual user or a system RFC user. Created by an SAP ERP system administrator.

The end user type is used, such as:

- Dialog user
- Background user

To use the standard processes that are delivered, customers must create individual end users.

Authorizations

The channel sales management for high tech scenario uses authorization provided by the SAP NetWeaver AS. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the application.

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

The channel sales management for high tech scenario uses the business partner information in SAP CRM to determine authorizations of users. This is done by maintaining the business partners in different roles and assigning these partners to the users. For more information, see the subsections below.

Standard Roles

The following table shows the standard roles that are used in the channel sales management for high tech scenario:

Table 348

Role	Description
CRM Business Partner Role – Employee	SAP Note 715494
CRM Business Partner Role – Contact Person, Internet User	SAP Note 715494

Standard Authorization Objects

The following table displays the security-relevant authorization objects that are used in the channel sales management for high tech scenario:

Table 349

Authorization Object	Authorization Field	Value	Description
CMS_SGEN	ACTVT	01, 03	Generation of rule schema
CMS_SMAINT	ACTVT	01, 03	Maintenance of rule schema
CMS_CIR	CHNL_PART SALES_ORG ACTVT	* * 02, 03, 43	Generation and processing of channel inventory reconciliation data
CMS_CI	ACVT CHNL_PART SALES_ORG	01, 02, 03, 06 * *	Maintenance of channel inventory data
CMS_IR	CHNL_PART SALES_ORG ACTVT	* * 02, 03, 43	Processing and maintenance of reported inventory data
CMS_RT_AUT	CHNL_PART SALES_ORG ACTVT	* * 02, 03, 43	Processing and maintenance of resale and claim data
CMS_PP_AUT	CHNL_PART SALES_ORG ACTVT	* * 01, 02, 03, 05, 06, 32	Generation and processing of price protection data
CMS_SI_AUT	CHNL_PART SALES_ORG ACTVT	* * 02, 03, 43	Processing and maintenance of sell-in data
CMS_TO	PARTNER ACVT	* 02	Generation of expected due list data and maintenance of transmission data

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). You must define the ACE rules and rights for channel sales management for high tech scenarios in in ACE

Customizing, because the rules in the SAP standard system are dummy rules. For more information, see the Access Control Engine [page 324] section.

Network and Communication Security

The network topology for the channel sales management for high tech scenario is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. The security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to the channel sales management for high tech scenario. For more information, see the Network and Communication Security [page 29] section.

Details that specifically apply to the application are described in the *Communication Channel Security* subsection below, which describes the communication paths and protocols used in the channel sales management for high tech scenario.

For more information, see the following sections in the *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide*:

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability*

Communication Channel Security

The following table lists the various communication channels that are used between the components used in the channel sales management for high tech scenario:

Table 350

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, conditions.
CRM server to ERP server	RFC	System ID, client, and host name, all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client, and host name, all application data	System information and ERP data
CRM server to Internet Pricing and Configurator (IPC) (Necessary only if IPC runs on a separate installation. See SAP Note 855455).	RFC	Pricing conditions	System information and CRM data
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data

Data Storage Security

Data is stored in database tables of SAP NetWeaver AS. Depending on the user role, the appropriate rights – read, write, change, and delete – are required. No addition data storage security is required.

7.2 Contracts and Chargeback for Pharmaceutical

SAP Customer Relationship Management (SAP CRM) enables the contracts and chargeback for pharmaceuticals scenario by including the following functions that are modeled as different applications:

- SAP Contract Management
- Chargeback claims processing
- Sell-in (sales to channel partner)
- Transmission management

These applications enable processing of the contracts and chargeback data. This includes creation of sales documents in SAP CRM and sales and invoicing documents in the back-end ERP system.

Why Is Security Necessary?

Security is necessary because the contracts and chargeback for pharmaceuticals scenario accesses data in SAP CRM. Information such as contract price information, member eligibility information, and chargeback claims is maintained in SAP CRM. It also leads to creation of sales documents in SAP CRM, which are replicated and invoiced in the back-end ERP system.

Security Aspects of Data, Data Flow and Processes

For dialog users, the communication between the WebClient UI and the SAP CRM back-end is established with the assignment to a business role and the corresponding PFCG role, communication protocol HTTP/HTTPS.

The sales documents created in the SAP CRM system are replicated by the system to the SAP ERP system, using an RFC call.

Business Roles

Table 351

Business Role	PFCG Role	Description
PHA_CLM	SAP_CRM_UIU_PHA_CLM	Life Sciences/Pharma CLM

User Administration and Authentication

The contracts and chargeback for pharmaceuticals scenario uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server (SAP NetWeaver AS). 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 this scenario.

In addition to these guidelines, the following section includes information about user administration and authentication that specifically applies to the contracts and chargeback for pharmaceuticals scenario.

This section lists the tools to use for user management, the types of users required, and the standard users that are delivered with the contracts and chargeback for pharmaceuticals scenario.

User Management

User management for the contracts and chargeback for pharmaceuticals scenario uses the mechanisms provided by the SAP NetWeaver AS ABAP, such as tools, user types, and password policies. For an overview of how these mechanisms apply, see the subsections below. In addition, we provide a list of the standard users required for using the contracts and chargeback for pharmaceuticals scenario.

User Management Tools

Table 352

Tool	Description	Prerequisites
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	SAP Library for SAP NetWeaver on SAP Help Portal at ▸ help.sap.com/nw_platform ▸ *<Choose relevant release>* ▸ *Application Help* ▸ *Function-Oriented View* ▸ *Security* ▸ *Identity Management* ▸ *User and Role Administration of Application Server ABAP* ▸ *Administration of Users and Roles* ▸.	None

User Types

Table 353

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access contracts and chargeback transactions. Created by an SAP CRM system administrator.
SAP CRM	N/A	No	System user	No	Mandatory user who can process background jobs.
ERP back end	End user	No	Dialog user	No	Mandatory user who can create sales and invoicing documents, posted into the sell-in application in the contracts and chargeback for pharmaceuticals scenario in SAP CRM.
ERP back end	N/A	No	System user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, the user can be an individual user or a system RFC user. Created by an SAP ERP system administrator.

Authorizations

The contracts and chargeback for pharmaceuticals scenario uses the authorization provided by SAP NetWeaver AS. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to this scenario.

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

In addition, the contracts and chargeback for pharmaceuticals scenario uses the business partner information in SAP CRM to determine the authorizations of a user. This is done by maintaining the business partners in different roles and assigning these partners to the users. For more information, see the subsections below.

Standard Roles

The following table shows the standard roles that are used in the contracts and chargeback for pharmaceuticals scenario:

Table 354

Role	Description
CRM Business Partner Role – Employee	See SAP Note 715494
CRM Business Partner Role – Contact Person, Internet User	See SAP Note 715494

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used in the contracts and chargeback for pharmaceuticals scenario:

Table 355

Authorization Object	Field	Value	Description
CMS_SGEN	ACTVT	01, 03	Generation of rule schema
CMS_SMAINT	ACTVT	01, 03	Maintenance of rule schema
CMS_CBAUTH	CHNL_PART VKORG ACTVT	* * 1, 2, 3	Processing and maintenance of chargeback claims
CMS_SI_AUT	CHNL_PART SALES_ORG ACTVT	* * 02, 03, 43	Processing and maintenance of sell-in data
CMS_TO	PARTNER ACVT	* 02	Maintenance of transmission data

Session Security Protection

For more information, see Session Security Protection [page 29].

Network and Communication Security

The network topology for the contracts and chargeback for pharmaceuticals scenario is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. The security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to the contracts and chargeback for pharmaceuticals scenario. For more information, see Network and Communication Security [page 29].

Details that specifically apply to this scenario are described in the *Communication Channel Security* subsection below. It describes the communication paths and protocols used in the contracts and chargeback for pharmaceuticals scenario.

For more information, see the following sections in the *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide*:

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability*

Communication Channel Security

The following table lists the various communication channels that are used between the components of the contracts and chargeback for pharmaceuticals scenario:

Table 356

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client, and host name, and all application data	System information and ERP data
CRM server to Internet Pricing and Configurator (IPC) (Necessary only if IPC runs on a separate installation. See SAP Note 855455 .)	RFC	Pricing conditions	System information and CRM data
CRM server to third-party supplier (transaction tax engine (TTE) or Vertex)	RFC	Tax data	System information and CRM data

7.3 Market Development Funds

Family Members (Payees/Channel Partners/Purchase Locations)

Authorizations

In the partner channel management scenario, maintenance and visibility of family members depend on the role of the user.

In the role corporate partner manager, the user is allowed to see family members who belong to the corporate partner of the logged-on user. Only the corporate partner manager can request for creation of payees, subchannel partners, and purchase locations, or assign existing channel partners to these roles. Subsequently, this needs to be approved by the brand owner. Upon approval, the corporate channel partner can maintain the partner structure and copy the purchase locations from the corporate node to the subnodes of the partner structure.

In the role partner manager in the case of a structured partner, users are only allowed to see their own channel partners in the partner structure and purchase locations as well as lower-level channel partners and purchase locations. Users are not allowed to see corporate payees.

In the role partner manager in the case of an unstructured partner, users are only allowed to see and maintain their own channel partners.

Therefore, application access has to be controlled by the access control engine (ACE) with the help of rules that are designed for special roles.

For more information about the access control rules in partner channel management, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *Basic Functions* > *CRM Access Control Engine*.

You must ensure that all necessary rules in ACE are activated:

- `MDF_BP_CORP_FAMILY`
- `MDF_BP_FAMILY_PAYEES`
- `MDF_BP_FMLY_3RDPARTY`
- `MDF_BP_MY_CHILDERN`

Third Parties

Authorizations

In the partner channel management scenario, maintenance and visibility of third parties depend on the role of the user.

Users with the corporate partner manager role can see third parties who belong to the corporate partner, as well as third parties who belong to the corporate channel partner's family members. Only the corporate partner manager is allowed to request the creation of corporate third parties. Subsequently, this needs to be approved by the brand owner.

In the role partner manager, in the case of a structured partner, users are only allowed to see their own third party and corporate third party.

In the role partner manager in the case of an unstructured partner, users are only allowed to see third parties of their own channel partners.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_BP_CCP_3PARTY_CO`
- `MDF_BP_CO_3RD_PARTY`

Corporate Channel Partners

Authorizations

In the partner channel management scenario, maintenance and visibility of corporate channel partners depends on the role of the user.

In the role corporate partner manager, users are allowed to see and maintain their own corporate channel partners.

In the role partner manager in the case of a structured partner, users are only allowed to see their own corporate channel partners.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that the `MDF_BP_MY_CORPORATE` rule in ACE is activated.

Channel Partner Contacts

Authorizations

In the partner channel management scenario, maintenance and visibility of channel partner contacts depend on the role of the user.

In the role corporate partner manager, users are allowed to see and maintain channel partner contacts of the corporate channel partner and see channel partner contacts that belong to the corporate channel partner’s family members.

In the role partner manager in the case of a structured partner, users are only allowed to see and maintain their own contacts and see channel partner contacts that belong to channel partners below them in the partner structure.

In the role partner manager in the case of an unstructured partner, users are only allowed to see and maintain their own contacts.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_CONTACT_READ_CCP`
- `MDF_CONTACT_READ_CP`

Programs

Authorizations

In the partner channel management scenario, programs are displayed only to the participating partners. The visibility of programs is controlled by the attribute *Visible for Partners*. The programs must be in one of the following statuses: *Released* or *Released, Locked* and *Released Approved*. The channel partner or the corporate channel partner of the user who is logged on must be a participating partner.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

For more information about the access control rules in partner channel management, see SAP Library on SAP Help Portal at ▶ help.sap.com/crm ▸ *<Choose a release>* ▸ *Application Help* ▸ *Basic Functions* ▸ *CRM Access Control Engine* ◀.

You must ensure that all necessary rules in ACE are activated:

- `MDF_PGM_FOR_COMPANY`
- `MDF_PGM_FOR_FAMILY`
- `MDF_PGM_FOR_HIER`

> **Note**
>
> Family and hierarchy rights for market development fund (MDF) programs are mutually exclusive. You can activate one or the other, but not both.

Checklist

Table 357

Feature	Check	How to Check
Control access of program/special program for different partner roles	Are the rules activated?	In Customizing for *Customer Relationship Management* under ▶ *Basic Functions* ▸ *Access Control Engine* ▸ *Activate/Deactivate Work Packages*

Feature	Check	How to Check
		and Rights ❯, choose the *Monitoring* tab and check whether all necessary rights have the status `ACTIVE`.

Special Programs

Authorizations

In the partner channel management scenario, special programs are displayed only to the participating partners. The visibility of programs/special programs is controlled by the attribute *Visible for Partners*. The programs/ special programs must be in one of the following statuses: *Released* or *Released, Locked* and *Released Approved*. The channel partner or the corporate channel partner of the user who is logged on must be a participating partner.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_SPG_FOR_COMPANY`
- `MDF_SPG_FOR_FAMILY`
- `MDF_SPG_FOR_HIER`

> **Note**
>
> Family and hierarchy rights for MDF special programs are mutually exclusive. You can activate only one or the other, but not both.

Checklist

Table 358

Feature	Check	How to Check
Control access of special program for different partner roles	Are the rules activated?	In Customizing for *Customer Relationship Management* under ❙▶ *Basic Functions* ❯ *Access Control Engine* ❯ *Activate/Deactivate Work Packages and Rights* ❯, choose the *Monitoring* tab and check whether all necessary rights have the status `ACTIVE`.

Initiative Templates

Authorizations

In the partner channel management scenario, initiative templates are displayed only to the channel partners.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that the `MDF_INITEMP_DISP_ALL` rule in ACE is activated.

Checklist

Table 359

Feature	Check	How to Check
Control access of program/special program for different partner roles	Are the rules activated?	In Customizing for *Customer Relationship Management* under ❙▶ *Basic Functions* ❯ *Access Control Engine* ❯ *Activate/Deactivate Work Packages*

Feature	Check	How to Check
		and Rights ▸, choose the *Monitoring* tab and check whether all necessary rights have the status `ACTIVE`.

Initiatives

Authorizations

In the partner channel management scenario, maintenance and visibility of initiatives depend on the role of the user.

In the role corporate partner manager, users are allowed to see initiatives that belong to family members of corporate channel partners.

In the role partner manager, users are only allowed to see initiatives that are assigned to the channel partner to which the user who is logged on belongs.

In the role partner manager, users are allowed to maintain initiatives that are assigned to one of the employees of the channel partner to which the user belongs and must not be in one of the following statuses: *Approved*, *Released*, *Archived*, *Can be archived*, *Submitted*, *Completed*, *Rejected*, and *Cancelled*. Users should only be able to set partners in the initiatives they are allowed to see.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all of necessary rules in ACE are activated:

- `MDF_INI_EMPLOYEE`
- `MDF_INI_MY_FAMILY`
- `MDF_INI_MY_COMPANY`

Checklist

Table 360

Feature	Check	How to Check
Control access of initiatives for different partner roles	Are the rules activated?	In Customizing for *Customer Relationship Management* under ▸ *Basic Functions* ▸ *Access Control Engine* ▸ *Activate/Deactivate Work Packages and Rights* ▸, choose the *Monitoring* tab and check whether all necessary rights have the status `ACTIVE`.

Funds

Authorizations

In the partner channel management scenario, maintenance and visibility of funds depend on the role of the user.

In the role corporate partner manager, users are allowed to see funds that are assigned directly to the corporate channel partner and any funds assigned to nodes below their node in the partner hierarchy structure. Corporate channel partners have change access to all funds assigned to their subnodes in their own partner structure (all their family funds but not their own funds).

In the role partner manager, users are allowed to see funds that are assigned directly to the channel partner to which the user who is logged on belongs and any funds assigned to nodes below their node in the partner hierarchy structure. In case of an unstructured channel partner, the user is allowed to see funds that are assigned directly to the channel partner to which the user who is logged on belongs.

Additionally, the funds need to be in one of the following statuses: *Released* or *Canceled*.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_FND_READ_FOR_MY`
- `MDF_FND_CHG_FOR_CCP`
- `MDF_FND_READ_FOR_CP`

Budget Postings

Authorizations

In the partner channel management scenario, maintenance and visibility of budget postings depend on the role of the user.

In the role corporate partner manager, users are allowed to see budget postings that belong to family members of the corporate channel partner.

In the role partner manager, users are only allowed to see budget postings that are assigned to the channel partner to which the user belongs.

In the role partner manager, the user is allowed to maintain budget postings of type *Extension and Renewal* that are assigned to one of the employees of the channel partner to which the user belongs. In addition, the budget postings must be in one of the following statuses: *Open at Partner*, *In Process at Partner* or *Rejected by Brand Owner*.

In the role partner manager, the user is allowed to maintain budget postings of type *Transfer and Automated Budget Transfer* that are assigned to one of the employees of the channel partner to which the user belongs.

In any partner role, budget postings of type *Update and Expire* are always display-only.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_BPO_FOR_EMPLOYEE`
- `MDF_BPO_FOR_FAMILY`
- `MDF_BPO_FOR_COMPANY`

Checklist

Table 361

Feature	Check	How to Check
Control access of budget postings for different partner roles	Are the rules activated?	In Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *Access Control Engine* › *Activate/Deactivate Work Packages and Rights* ◀, choose the *Monitoring* tab and check whether all necessary rights have the status `ACTIVE`.

Claims

Authorizations

In the partner channel management scenario, maintenance and visibility of claims depend on the role of the user.

In the role corporate partner manager, the user is allowed to see claims that belong to family members of the corporate channel partner.

In the role partner manager, the user is only allowed to see claims that are assigned to the channel partner to which the user belongs.

In the role partner manager, the user is allowed to maintain claims that are assigned to one of the employees of the channel partner to which the user belongs and must be in one of the following statuses: *Open at Partner*, *In Process at Partner*, and *Transferred to Partner*. Users should only be able to set partners in the claims they are allowed to see.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_CLAIM_FOR_OWN`
- `MDF_CLAIM_FOR_FAMILY`
- `MDF_CLAIM_FOR_COMPANY`

Reservations

Authorizations

In the partner channel management scenario, maintenance and visibility of reservations depend on the role of the user.

In the role corporate partner manager, the user is allowed to see reservations that belong to family members of the corporate channel partner.

In the role partner manager, the user is only allowed to see reservations that are assigned to the channel partner to which the user belongs.

In the role partner manager, the user is allowed to maintain reservations that are assigned to one of the employees of the channel partner to which the user belongs and must be in one of the following statuses: *Open at Partner*, *In Process at Partner*, or *Transferred to Partner*. Users should only be able to set partners in the reservations they are allowed to see.

Therefore, application access has to be controlled by ACE with the help of rules that are designed for special roles.

You must ensure that all necessary rules in ACE are activated:

- `MDF_RESV_EMP`
- `MDF_RESV_FAMILY`
- `MDF_RESV_COMPANY`

8 SAP CRM Powered by SAP NetWeaver

8.1 CRM Server

This section explains the security aspects associated with the data present in the Customer Relationship Management (CRM) Server. The middleware for SAP CRM, which is an integral part of the CRM server, is based on the following components:

- SAP CRM server
- SAP ERP

Why Is Security Necessary?

The data synchronization within the CRM landscape (CRM server, ERP system, connectivity to Business Intelligence (BI) and CRM mobile clients) is provided by the middleware in SAP CRM. The data exchanged between the different components encapsulate the main business data (orders, business partners, sales conditions, and so on). This makes the data security in that area a critical topic that must be considered while setting up and customizing the system landscape. It is necessary to establish a well-defined authorization concept that assigns appropriate roles with restricted authorizations to different user groups in your company. For example, users and administrators of the administration console have different roles: the system administrator has full access to the queue monitors, restart ability, and deletion ability in the business document (BDoc) message monitoring tools.

Important SAP Notes

Table 362

SAP Note Number	Short Text	Comment
338537	Remote function call (RFC) user authorization for data exchange between ERP and CRM	This note provides recommendations about how to define the authorization concept for data exchange between the ERP and CRM servers. This is applicable to the main applications.
1425666	CRM Middleware	This note enhances the security of CRM Middleware code lines in such a way that unauthorized users cannot view or modify application content.
1501685	Table `CRMATAB` is empty	This SAP Note provides instructions on filling the table `CRMATAB` and is related to SAP Note 1498111.
1498111	No authorization for data selection in initial load	This SAP Note provides instructions on enhancing the security of CRM Middleware in terms of the data selection in the initial load.

For more information about security-relevant SAP Notes, see

User Administration and Authentication

User Management

The data synchronization between the CRM server and SAP ERP and within the CRM server is based on the RFC protocol. To enable the RFC connection between two systems or clients, a user is required. The use of a communication user (also known as RFC user) is important in a security-sensitive environment. The authorizations assigned to that user must be well-defined and restrictive. The type of user and related authorizations depend on your security requirements. For more information about SAP CRM user authorizations, see SAP Note 338537.

The following table lists the users that must be created to enable the data exchange:

Standard Users

Table 363

System	User	Type	Default Password	Description
SAP ERP	User for the CRM server and client	Communication user	To be set by the administrator	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Create RFC Users* ◀.
CRM server	User for the ERP server and client	Communication user	To be set by the administrator	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Create RFC Users* ◀.
CRM server	Replication and realignment user This user is applicable only for field applications scenarios.	Communication user	To be set by the administrator	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Define RFC Destinations* ◀.

Authorizations

Middleware in SAP CRM delivers different roles that are assigned to the middleware administrator, middleware developers, and CRM middleware consultants. There are also additional roles based on the tools to be used by the different project members (CRM project team, consultants, developers, administrator, power users, and so on). An authorization concept must be defined according to your requirements and to the team structure. We recommend that you have well-defined roles in the first phase of the project. Furthermore, assign the person responsible for the system and SAP support users full access to the main tools and transactions. The roles delivered by SAP are described in the sections below.

General CRM Middleware Roles

The following table lists the composite roles that are available for middleware in SAP CRM:

Table 364

Role	Description
SAP_CRM_MW_ADM	SAP CRM Middleware Administrator This role allows you to start all the transactions associated with the administration of the CRM server. This role is assigned to the administrator of the middleware in SAP CRM or SAP support. However, to ensure proper system monitoring, this role must be assigned only to system administrators in the productive systems.
SAP_CRM_MW_CUSTOMIZING	Customizing Steps for CRM Middleware (single role) This role allows you to customize the middleware in SAP CRM. This role is assigned to consultants and is primarily required during the initial setup of the CRM server.
SAP_CRM_MW_DEV	SAP CRM Middleware Developer This role is primarily required in the development system. However, during a crisis situation, this role can be used in the production system.

Note

Each role contains single roles. For more information, see the profile generator (PFCG) transaction.

The transactions along with their assigned roles are as follows:

BDoc Summary, Transactions R3AC1, R3AC3, R3AC5

Table 365

Role	Description
SAP_CRM_MW_ADP_ADMINISTRATOR	Authorizations for starting an initial load
SAP_CRM_MW_ADP_CUSTOMIZER	Authorizations for transactions R3AC1, R3AC3, and R3AC5

BDoc Modeler, Transaction SBDM

The following table lists the roles delivered by SAP:

Table 366

Role	Description
SAP_CRM_BDM_ACTIVATE_ALL	BDoc Modeler – Activate all BDoc types
SAP_CRM_BDM_CHANGE_ALL	BDoc Modeler – Change all BDoc types
SAP_CRM_BDM_CHECK_ALL	BDoc Modeler – Check all BDoc types
SAP_CRM_BDM_DELETE_ALL	BDoc Modeler – Delete all BDoc types
SAP_CRM_BDM_DISPLAY_ALL	BDoc Modeler – Display all BDoc types
SAP_CRM_BDM_GENERATE_ALL	BDoc Modeler – Generate all BDoc types
SAP_CRM_BDM_RELEASE_ALL	BDoc Modeler – Release all BDoc types
SAP_CRM_BDM_SYNC_BDOCS	BDoc Modeler – Synchronization BDoc types

Role	Description
`SAP_CRM_BDM_MESSAGING_BDOCS`	BDoc Modeler – Messaging BDoc types
`SAP_CRM_BDM_MOBILE_APPL_BDOCS`	BDoc Modeler – Mobile Application BDoc types

BDoc Message Summary, Transaction SMW01

BDoc messages are data containers used during the data synchronization by middleware in SAP CRM. The business data can be accessed by viewing the classical or the extended data part of the BDoc message in the corresponding BDoc messages monitoring tool: *Display BDoc Messages* (transaction `SMW01`). We recommend that you restrict the access to transaction `SMW01` in the production system to the system administrators, SAP support, and the responsible project leads or members only. Remove the authorizations for transaction `SMW01` for all other dialog users. In most cases, developers have full access to the development and test systems. We also recommend that you restrict the authorizations to reprocessing features and deletion features for the same transaction. The incorrect use of these features can lead to data inconsistencies in the system landscape.

The following table lists the roles that are available for BDoc processing:

Table 367

Role	Description
`SAP_CRM_MWSMW_DELETE`	Check authorization to delete BDoc messages
`SAP_CRM_MWSMW_RETRY`	Check authorization to retry the processing of BDoc messages

qRFC Queues, Transactions SMQ1/SMQ2

To optimize the use of the system resources and the parallelization of data processing, the data synchronization uses the SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP) queue mechanisms. The data is partly readable in the queues. You must prevent access to the data in these queued remote function call (qRFC) queues. To do this, remove the authorizations for *qRFC Monitor (Outbound Queue)* (transaction `SMQ1`) and *qRFC Monitor (Inbound Queue)* (transaction `SMQ2`) for all the dialog users. Only administrators, CRM project leads, and SAP support need to start these transactions. Deleting queue entries is also critical (it leads to severe data inconsistencies in the system landscape) and has to be avoided. Authorizations can be limited. It is possible to disable the deletion of entries from the inbound or outbound queues. For information about how to activate the authorization check for deletion from the RFC queues, see SAP Note 93254.

Follow the instructions provided in SAP Note 622722 to ensure that the inbound queues are processed by a user with the required authorizations. For all the other dialog users, specify power users who are aware of the consequences of deleting a queue entry or making stop entries.

Replication and Realignment (R&R) Queue Processing, Transaction SMOHQUEUE

This section is valid for the field applications scenario only. If the processing of the replication and realignment queues that provide data to the mobile clients extends for a long period of time, do not delete the entries present in the queues. Otherwise, it is a time-consuming process to correct the inconsistencies in the lookup tables because the data volume increases significantly and in some specific instances, a complete new processing of all the object instances is required. If the inconsistencies in data distribution are caused by customers due to unauthorized interference in the queue processing, then SAP is not responsible for these inconsistencies. We recommend that you follow stringent measures before assigning authorizations for *Monitor R&R Queues* (transaction `SMOHQUEUE`). The corresponding authorization object is `CRM_MW_RR` and authorizations to delete entries from these queues must be granted only to administrators of the CRM server.

Standard Authorization Objects

It is possible that instead of using the standard roles, single authorization objects are required. The following table lists the relevant authorization objects:

Table 368

Authorization Object	Description
`CRM_MW_FC`	Flow control
`CMW_BDM`	BDoc modeler
`CMW_CRMADP`	CRM adapter repository
`CMW_GEN`	CRM middleware generation
`CRM_MW_AC`	Admin console
`CRM_MW_BDM`	BDoc modeler
`CRM_MW_DC`	Data collector/extractor
`CRM_MW_RR`	R&R queue administration

For more information about the authorization objects, see the corresponding field help.

Network and Communication Security

Communication Destinations

Table 369

Destination	Delivered?	Type	User, Authorizations	Description
RFC destinations for the ERP target systems (SAP ERP, SAP NetWeaver BW, SAP Advanced Planning & Optimization (SAP APO))	No	RFC connection	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Create RFC Users* ◀.	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Define RFC Destinations* ◀. For more information, see SAP Note 338537.
RFC destinations for non-ERP target systems	No	RFC destination	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Create RFC Users* ◀.	See the Customizing documentation in Customizing for *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Define RFC Destinations* ◀.

Checklist

Table 370

Feature	Check	How to Check
Data synchronization in the system landscape	RFC destinations and RFC users	See the *Communication Destinations* and *User Management* subsections above.
Authorization concept	Roles and authorization objects assigned to the different user groups	See the *Authorizations* and *Standard Authorization Objects* subsections above.
Data protection and consistency	BDoc messages: transaction `SMW01` Queuing: transactions `SMQ1` and `SMQ2` Data replication: transaction `SMOHQUEUE` (for field applications only)	See the *BDoc Message Summary, qRFC Queues, and Replication* and *Realignment (R&R) Queue Processing* subsections above.

8.2 Software Agent Framework

This section is for the compilation service and search service of the software agent framework (application component CRM-BF-SAF).

Related Security Guides

Table 371

Application	Guide	Most-Relevant Sections or Specific Restrictions
Interaction center WebClient (IC WebClient)	*SAP Customer Relationship Management Security Guide*	*Component-Specific Guidelines: Interaction Center*
Search and Classification (TREX)	*Search and Classification (TREX) Security Guide*	SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform ▶ *<Choose relevant release>* ▶ *Security Information* ▶ *Security Guide* ▶ *Security Guides for SAP NetWeaver Functional Units* ▶ *Search and Classification (TREX) Security Guide*

Why Is Security Necessary?

Data protection is important for this application because the software agent framework (SAF) can integrate various knowledge bases, some of which could contain sensitive information such as business partner details.

User Administration and Authentication

User Management

The SAF has no user management tools of its own. To maintain users, you can use the standard ABAP *User Maintenance* (`SU01`) transaction.

User

Table 372

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Knowledge engineer	No	Dialog	No	There are different ways to access the SAF's Indexes Business Server Page (BSP) application. To access it using a URL or from SAP CRM directly, a standard CRM user is sufficient.

Network and Communication Security

Communication Channel Security

TREX's ABAP application programming interface (API) communicates with the TREX server using TCP/IP communication supported by SAP's standard remote function call (RFC) definition. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Search and Classification (TREX) Security Guide* ◀.

Network Security

The SAF compilation service has no firewall settings of its own.

Communication Destinations

The RFC destination to the TREX server is required and, after the TREX server is installed, the RFC destination should be configured in SAP CRM in Customizing for *Customer Relationship Management* under ▶ *Enterprise Intelligence* › *Software Agent Framework* › *Configure RFC Destinations* ◀.

Data Storage Security

All data requires protection to avoid unauthorized access. As an ABAP component, the SAF integrates TREX's ABAP API and SAF business objects or documents. The SAF provides search and index services for different business applications, such as the interaction center WebClient's knowledge search or e-service. Only users with access to the business application can use SAF functions. Furthermore, any content access through a business application using the SAF, such as view details, is controlled by individual business objects, such as problems and solutions in the solution database (SDB).

Access control can be administrated by SAP's standard authorization and SAF information security. For information about SAF information security, see the following:

- SAP Library on SAP Help Portal at ▶ help.sap.com/crm › *<Choose a release>* › *Application Help* › *Interaction Center* › *Software Agent Framework (SAF)* › *Generic Information Security* ◀
- Customizing for *Customer Relationship Management* under ▶ *Enterprise Intelligence* › *Software Agent Framework* › *Business Add-Ins (BAdIs)* › *BAdI: Information Security* ◀

Stored Data

Table 373

Data	Stored Where	Stored When	Type of Access	Protected by Access Control
Knowledge bases	SAP system	Knowledge base maintenance	Read/write/delete/change	Yes – Access required to SAP CRM
Knowledge base indexes (compilation service)	TREX	Indexing	Write/delete/change	Yes – Access required to index BSP application or to TREX server
Knowledge base indexes (search service)	TREX	User interaction	Read	Yes – Access required to SAP CRM or to TREX server
Compilation status/time stamp	SAP system	Indexing/clustering	Read/write/delete/change	Yes – Access required to index BSP application
Clustering result	SAP system	Clustering	Read/write/delete/change	Yes – Access required to index BSP application
SAF Customizing	SAP CRM	SAF post installation	Read/write/delete/change	Yes – Access required to Customizing
Feedback (search service)	SAP CRM	User interaction	Read/write/change	Yes – Access required to Customizing

There are no other places in which data is temporarily stored.

The compilation service supports or requires a Web browser as the user interface. The search service does not require a Web browser.

Cookies are not used to store data at the front end.

No further data is stored on the client.

Other Security-Relevant Information

This application does not use active code on the front end.

8.3 Solution Database

Related Security Guides

Table 374

Application	Guide
Software agent framework	*SAP Customer Relationship Management Security Guide*
Content management	*Knowledge Management Security Guide*

Application	Guide
	See SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Application Help* > *Function-Oriented View* : Search for *Knowledge Management Security Guide*.

Why Is Security Necessary?

Information such as company data and employee data stored in the solution database (SDB) should not be accessible to everyone. Therefore, it is necessary to restrict access to certain information. In the SDB itself, problem and solution records can be accessed only using the SDB's search interface. When the SDB is searched from another application (for example, from the interaction center WebClient (IC WebClient) knowledge search), there is a security risk if the application is allowed to access the entire SDB. For this reason, access can be controlled according to user by using information security. For more information about information security, see the *User Management* subsection below.

User Administration and Authentication

User Management

Table 375

Tool	Description
Change Information Security Profile (transaction `CRMD_SDB_PRMN`)	See below
Assign Profile to User (transaction `CRMD_SDB_PROF`)	See below

SDB information security is an online maintenance tool for knowledge administrators to restrict the access of certain users to only certain categories of information when users search the SDB using the following:

- Knowledge search in the interaction center WebClient (IC WebClient)
- Standalone knowledge search: *Knowledge Search* (transaction `CRMM_SEARCH`)
- Frequently asked questions (FAQs) and solution search in Internet customer self-service (ICSS)

For example, you may want to allow customers searching the SDB using ICSS to access only information for external users, not to retrieve documents flagged for internal use only.

Information security is achieved by the use of problem profiles, solution profiles, and group profiles. The set of problems and solutions displayed is determined by the values of attributes such as the problem type and validation category. For example, you could specify that the profile *Guest* is allowed to retrieve only documents belonging to problem type *A* and validation category *Guest*.

Information Security Profiles

Table 376

Problem Profile	Solution Profile	Group Profile
Individual profile containing a set of values for one or more of the following attributes: • Problem type • Problem subtype • Application area • Validation category	Individual profile containing a set of values for one or more of the following attributes: • Solution type • Solution subtype • System status • User status	Collection of individual problem and solution profiles. It allows the user to access all problems and solutions matching at least one of its individual profiles.

Problem Profile	Solution Profile	Group Profile
- Priority type and level - System status - User status - Subject profile		

There is no additional user management for information security. The standard SAP users are used. The individual profiles and group profiles are stored and delivered as customized data of the SDB.

User Data Synchronization

It is not necessary to synchronize the user data with other data sources.

Authorizations

A standard CRM user is sufficient.

Data Storage Security

There are no special data storage security requirements because it is sufficient that security is ensured by default settings.

Records are stored in the database of SAP CRM as master data. Individual information security profiles and group information security profiles are stored and delivered as customized data of the SDB (see the *User Management* section above).

Other Security-Relevant Information

This application does not use active code on the front end.

8.4 UI Framework

User Administration and Authentication

User Management

Table 377

Tool	Description
User Maintenance (`SU01`) transaction	You must create and store all users in SAP Customer Relationship Management (SAP CRM) and the back-end system. To use Web applications, all customers must first have an account created using the *User Maintenance* (`SU01`) transaction.

User authentication is performed by using standard tools of SAP NetWeaver Application Server (SAP NetWeaver AS) along with the connected SAP ERP system (CRM server).

Logon Procedure

SAP Customer Relationship Management (SAP CRM) uses standard logon procedures provided by the Internet communication framework of SAP NetWeaver AS: *Maintain Services* (transaction `SICF`).

The logon procedure is configured in the following locations:

- `/default_host/sap/bc/bsp/sap/crm_ui_start`

  - Default form-based logon procedure (user/password)
  - Function for changing passwords
- `/default_host/sap/crm_logon` (alias of 1)
  - Form-based logon procedure (user/password/client/language)
  - Function for changing passwords

If you want to change the default logon procedure, create your own alias of service `/default_host/sap/bc/bsp/sap/crm_ui_start` and make the changes there. Do not change the SAP service/alias.

For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* : Search for *Activating and Deactivating ICF Services*.

For more information about ICF security, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for Connectivity and Interoperability Technologies* › *RFC/ICF Security Guide* .

Authentication When Using SAP CRM Search Modeling Workbench

The enterprise search modeling workbench (transaction `CRM_ES_WB`) in SAP CRM is an SAP GUI application. Users are authenticated when they log on to the system.

Authentication When Using Atom Feed

When `crm_feed` service is accessed, the standard user authentication is performed. This implies that the Atom reader used must support feeds requiring authentication.

Once the user is authenticated, the system sends the corresponding CRM data back to the Atom reader under the following conditions:

- The user has the right to use the feed, as checked with the authorization object S_WCF_FEED.
- The user is assigned to the CRM business role for which the feed is requested.
- The authority checks allow the user to access the corresponding data.

  For more information, see the *Authorizations* section below.

An individual entry returned by the CRM feed can contain a direct link to a business object on the WebClient UI. The user can click that link to open the standard CRM application in the Web browser. The security standards are the same as when the user accesses the WebClient UI in its Web browser and navigates to the business object.

Authorizations

Authorization Concept Overview

In the CRM role concept, there is a dependency between business roles and PFCG roles. Each business role has a corresponding PFCG role containing only those authorization objects needed to fulfill the task defined in the business role. This section describes the parts involved in creating custom PFCG roles for business roles.

For more information about setting up authorizations for business roles, see Customizing for *Customer Relationship Management* under *Business Roles* › *Overview* .

The figure below, along with the table that follows, illustrates dependencies between the following:

- PFCG role menu and the business role
- User and the PFCG role

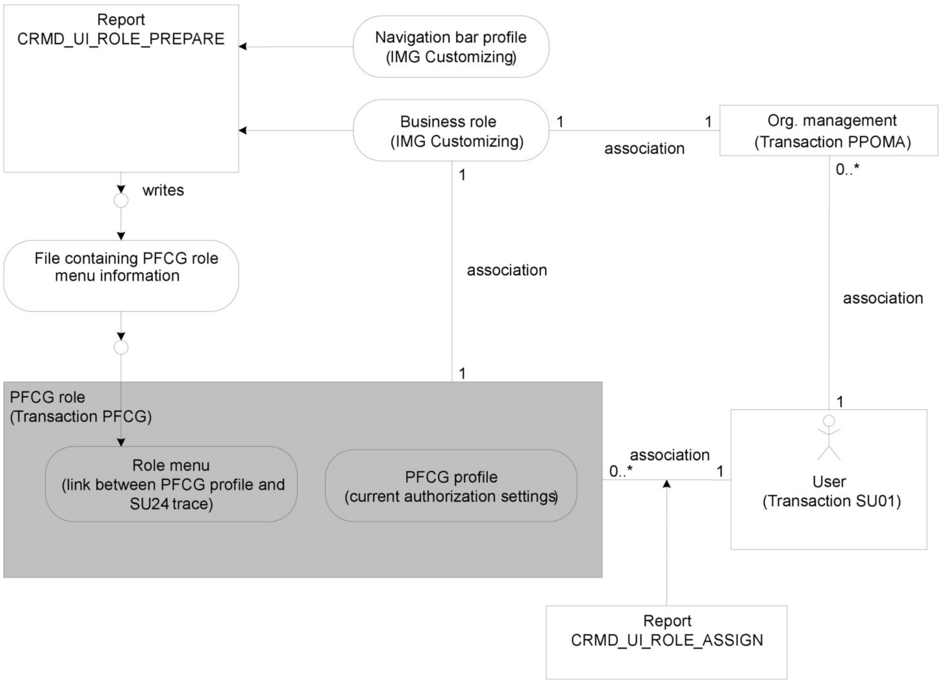


Figure 28: Role Dependencies

Table 378

Component	Description
User	SAP CRM uses standard user maintenance (SU01). Authorizations are provided using PFCG profiles and roles assigned to the users.
Organizational management	Users are indirectly assigned to business roles using organizational management. If a position in organizational management is assigned to a business role using info type *Business Role*, then in turn, all users are assigned to this business role as well. For more information about other ways to assign business roles, see the *Determination of Business Roles* section below.
Navigation bar profile	Used to define work centers, logical links, and so on. Provides common settings used in business roles.
Business role	Uses and adopts the navigation bar profile to the needs of particular business functions. For example, work centers can be turned off. There is usually an assignment to one PFCG role.
Report CRMD_UI_ROLE_ASSIGN	Assigns PFCG roles to users based on user assignments in organizational management (positions in organizational management are assigned in turn to business roles).
PFCG role	Contains authorizations tailored to the business role. The authorizations are retrieved from SU22/SU24 traces (at SAP customers), based on the PFCG role menu.

Component	Description
	⚠ Caution Every user must be assigned to the PFCG role SAP_CRM_UIU_FRAMEWORK, in addition to the business role-specific PFCG role. Usually there is a 1:1 relation between business roles and PFCG roles. There are, however, cases where this is not suitable. You can then use Customizing for business roles to assign the same PFCG role to several business roles or to omit a PFCG role.
PFCG role menu	This menu is imported from a file created by report CRMD_UI_ROLE_PREPARE in the PFCG transaction. Each role menu option is linked to an SU22/SU24 trace. The menu contains all traces and in turn all the authorizations needed to run a specific business role.
Report CRMD_UI_ROLE_PREPARE	The report creates the role menu file based on the settings in Customizing. This information represents the link between the business role settings and the SU24 traces.

The figure below, along with the table that follows, illustrates dependencies between the following:

- PFCG role and the SU22/SU24 traces
- PFCG role and the WebClient-based application

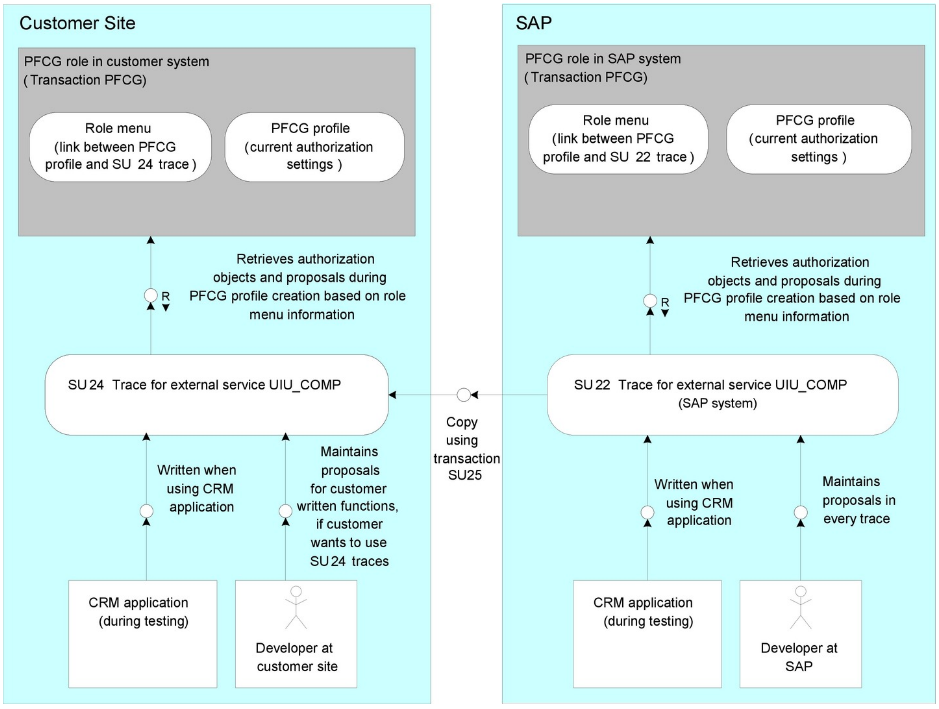


Figure 29: Dependencies

Table 379

Component	Description
PFCG profile	Contains authorization objects needed for a particular business role. The profile retrieves authorization objects from the SU22/SU24 trace during profile creation. Only the traces connected to the PFCG role by the role menu are read.
SU22 trace	Authorization traces delivered by SAP. The WebClient UI uses the external trace type UIU_COMP.
SU24 trace	Authorization traces maintained by the customer. These traces are copied from the SAP namespace (SU22) using transaction SU25.
CRM application	Available UI functions are controlled using business role Customizing. Authorizations are controlled by PFCG roles. SU22 (at SAP) and SU24 (at the customer) traces are written if they are activated when the application performs an authorization check. To activate or deactivate a trace, use transaction RZ11: auth/authorization_trace = Y: active auth/authorization_trace = N: inactive To optimize the coverage of the authorization check in the SU22 and SU24 traces, execute a larger number of functions in the application.

Determination of Business Roles

To use the WebClient UI, the user needs to have a business role assigned to his or her user. Business roles are determined in the following order:

1. Check whether a single business role is assigned using the user parameter CRM_UI_PROFILE. This setting overrules any other role assignments.
2. Check whether there are business roles assigned using *Organizational Management*.
3. If neither of the above cases are true, the system determines the PFCG roles assigned to the user and checks whether they are linked to a business role. If this is the case, this business role is used.

Web-Based Business Role Customizing

It is possible to customize business roles using the WebClient UI. For more information, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *WebClient UI Framework* > *Business Roles*.

Application Enhancement Tool

The application enhancement tool is defined in the *Administration* work center (work center link groups: CT-ADM-SR). Activating the *Administration* work center in any business role requires an update of the PFCG role.

The application enhancement tool provides a standard PFCG role with the name SAP_AXT_EXTENSIBILITY_ADMIN, which contains the entire needed authorization object from the SU22 trace.

To use SAP CRM interactive reporting, the user needs PFCG role `SAP_CRM_OR_USER` in the business intelligence (BI) client and in the CRM client. To activate the enhancement in interactive reporting, the user needs PFCG role `SAP_CRM_OR_ACTIVATE` in the BI client.

To use the *Application Reference* field type, ensure that users accessing fields of that type have application-specific authorization objects. For more information about application-specific authorization objects, see the relevant application-specific section.

To use tags from the central data storage in calculated fields or the embedding mechanism, you need the authorization object `TAG_ATB`.

To define calculated fields from the Application Enhancement Tool, no additional authorization is needed. For support or administration of Business Rule Framework plus (BRFplus) formula, you need the `SAP_BC_FDT_ADMINISTRATOR` role.

Central Sharing Tool: Prevention of Unauthorized Access to Items by Recipients

The central sharing tool is a feature that allows users with special privileges to share their tags, favorite objects, saved searches, and reports with other users, business roles, an organizational unit, or a position in a business role.

Technical and authorization checks are run to prevent recipients from accessing items, such as saved searches, that they would not be otherwise allowed to access. A two-level approach is used.

First, when the object is shared, all technically possible checks are run to verify that the recipients have the authorization/option to view the shared items. If a problem is detected, sharing is not possible.

Secondly, before the items are displayed in the recipient's share box, all the remaining checks are run. If any authorization problems are detected, the corresponding item is not displayed.

The following table is a description of the checks that are run:

Table 380

Object	Description	Sharing Time	Recipient Display Time
Saved Search	The user needs to navigate to the relevant search page or result page. Criteria are shared, not the result. It is not necessary to check each result entity. When the actual search is executed, the results of the authorization checks dictate whether or not the BOL returns the entity.	Is the required Customizing for navigation available?	Is the required Customizing for navigation available?
Favorites	The user needs to be able to dynamically navigate to the object overview page and to display the corresponding entity.	Is the required Customizing for navigation available? (Navigation to mixed list and to the object overview page)	Is the required Customizing for navigation available? (Navigation to mixed list and to the object overview page) Can the current user access the corresponding BOL entity?
Tags	The tag itself is shared, not the tagged object. It is not necessary to check each	Is the required Customizing for navigation available? (Navigation to mixed list)	Is the required Customizing for navigation available? (Navigation to mixed list)

Object	Description	Sharing Time	Recipient Display Time
	tagged entity. When the mixed list is called, the objects are filtered to display only those that the user is allowed to see.		
Reports	If the *Logical Link* report is customized for a business role, the report can be displayed by all users of that business role. There is only an authorization check on the content of the report. Different users might see different data in the report based on their authorizations.	Is the required Customizing for navigation available? (Navigation to the logical link)	Is the required Customizing for navigation available? Navigation to the logical link)

The BOL implementation authorization check is used to check if the recipient has access to a BOL entity.

Central Sharing Tool: Prevention of Unauthorized Access to Items by Sharers

The sharer can select the following as recipients:

- Organizational units
- Positions within an organizational unit
- Business roles
- Individual users

The following authorization objects are used to control access by the sharers to only those recipients to whom they were granted access.

Table 381

Audience Type	Authorization Object	Field/Suggested Values
Users	S_USER_GRP	ACTVT/03 (Display)
Business role	S_TABU_DIS	S_USER_GRP (Display) DICBERCLS/CRMC
Organizational units and positions	PLOG	PPFCODE/DISP PLVAR/01 OTYPE/O, S, US

Standard Roles

Table 382

Role	Role Description
SAP_CRM_UIU_FRAMEWORK	This role is a special role that is assigned to every user. It contains the authorizations that are necessary to use the SAP CRM framework.

Authorization Objects

The WebClient UI framework includes the following authorization objects:

Table 383

Used By	Authorization Object	Description
UI framework	UIU_COMP	Restricts access to applications at the component level. Only authorized users can launch the WebClient UI.
UI Customizing	CRM_CONFIG	The authorization object CRM_CONFIG is used to restrict authorization for UI configuration based on component name, BSP view name, UI object type, and role configuration key.
Transaction launcher	C_LL_TGT	Controls authorizations of logical links of type C (launch transaction) and D (BI report).
Web service tool	CRM_WST	Controls access to the Web service tool in SAP CRM.
Application Enhancement Tool	S_DEVELOP	The authorization object S_DEVELOP is used in the application enhancement tool to restrict general authorization for enhancement generation.
	S_CTS_ADMI	This authorization object is needed to transport enhancement.
	S_CTS_SADM	This authorization object is needed to transport enhancement.
	S_ICF_ADM	This authorization object is needed to generate UI component for enhancement.
	S_RO_OSOA	The authorization object S_RO_SOA is used in the application enhancement tool to restrict authorization for generation of data source.
	S_TRANSPRT	The authorization object S_TRANSPRT is used in the application enhancement tool to create new transport request or new task.
	S_TCODE	This authorization object is needed to regenerate invalid load.
	TAG_ATB	This authorization object is needed to make use of the tag attribute.
	S_TABU_DIS	The authorization object S_TABU_DIS is used in the application enhancement tool to restrict authorization for generation of table entry.
Rapid Application Tool	S_CTS_ADMI	Needed to transport rapid applications
	S_CTS_SADM	Needed to transport rapid applications
	S_DEVELOP	This authorization object is used in the embedding tool to generate rapid applications.
	S_ICF_ADM	This authorization object is needed to generate UIs for rapid applications.
	S_TABU_DIS	This authorization object is used in the embedding tool to restrict authorization for generation of table entries.

Used By	Authorization Object	Description
	`S_TCODE`	This authorization object is within the generation framework to regenerate invalid load.
	`TAG_ATB`	This authorization object is needed to make use of the tag attribute.
	`S_TRANSPRT`	This authorization object is used in the embedding tool to create new transport requests or new tasks.
Web Service Consumption Tool	`CRM_WSC`	Controls access to the Web Service Consumption Tool. For more information, see SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Basic Functions* › *Web Services* › *Web Service Consumption*.
	`S_CTS_ADMI`	This authorization object is needed to transport the generated objects.
	`S_CTS_SADM`	This authorization object is needed to transport the generated objects.
	`S_DATASET`	This authorization object is needed to access the locally saved WSDL file.
	`S_DEVELOP`	This authorization object is used to generate the objects.
	`S_TRANSPRT`	This authorization object is used to create new transport requests or new tasks.
Enterprise search integration	`S_DEVELOP`	Restricts access to the enterprise search modeling workbench
	`S_ESH_ADM`	Restricts transfer of CRM models to enterprise search to authorized users
	`S_TABU_DIS`	Restricts client copy of CRM models to authorized users
	`S_TRANSPRT`	Restricts maintenance of Customizing transports containing the CRM models to authorized users
Atom feed	`S_WCF_FEED`	This authorization object is used to restrict access to the feed function in SAP CRM.

For more information, see the object documentation using *Maintain the Authorization Objects* (transaction `SU21`) and the UI configuration guide.

The main business-related authority checks are done by business objects within the business object layer (BOL) and by applications.

For more information about authority checks and working with authorization objects, see the following:

- *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide*
- SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Basic Functions* › *CRM Access Control Engine*.

Important SAP Notes

Table 384

SAP Note Number	Title
1251796	Authorization Role of Application Enhancement Tool

Authorizations of Atom Feeds

The authorization object `WCF_FEED` is used to authorize or forbid the usage of the Atom feed feature in SAP CRM. The following authorization check is performed to verify the rights of the user to access the feed:

Syntax

```
AUTHORITY-CHECK OBJECT 'WCF_FEED'
ID 'FEED_ID' FIELD iv_feed_id
ID 'ACTVT' FIELD '03'.
```

In other words, the user needs display rights to access the feed with ID iv_feed_id. So far only the feed with ID `DEFAULT` is delivered, so the only value used for iv_feed_id variable is `DEFAULT`.

In addition to this authorization check, SAP CRM standard authorization checks are used in CRM feeds. This means that when a given type of data is being retrieved, such as an alert, the authority checks performed are the same ones used when data is accessed in the standard WebClient UI (for example, in worklist alerts).

Protection of User Parameters

We recommend that you prevent users from adding new parameters or changing user parameters in the profile.

Note

If users have access to the WebClient UI, but not the SAP GUI, users should not be able to use the*Maintain User Profile* (`SU3`) transaction to change user parameters.

Network and Communication Security

Communication Channel Security

The following table shows the general communication paths used, the protocol used for the connection, and the type of data transferred.

Table 385

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Browser to application	HTTP/HTTPS (secure)	All application data	Passwords and other sensitive data
CRM server to CRM server or ERP server	Remote function call (RFC)/ Secure network communication (SNC) (secure)	System ID, client name, and host name; all application data	System information and application data
Atom feeds	HTTPS	Business data	The SICF `service /sap/crm/crm_feed` requires SSL. This means that the Atom

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
			reader that is used must support HTTPS access.
Communication between application enhancement tool and business intelligence (BI) client	RFC	Used to connect from the application enhancement tool to the BI client to extend the online transaction processing system (OLTP) reporting for interactive reporting in SAP CRM.	N/A
Communication between WebClient UI framework and SAP NetWeaver Portal	RFC	Used to connect from the CRM back end to SAP NetWeaver Portal to call the object-based navigation Web service and to detect whether there is a portal target iView (portlet) for a given portal business object and operation. For more information, see Customizing for *Customer Relationship Management* under *UI Framework* > *Portal Integration*.	N/A
Communication between SAP CRM and SAP NetWeaver enterprise search	TCP/IP	Used for all enterprise search-related activities in SAP CRM such as transfer of CRM models, extraction of CRM templates, and search.	N/A

Communication Channel Security: Virus Scan Profiles

For information about virus scan profiles, see the Network and Communication Security [page 29] section.

Secure Sockets Layer (SSL)

The interaction between the CRM UI framework and SSL is limited. You use SSL to extend the capabilities of HTTP.

The SAP NetWeaver AS and SSL do not interact with the Web applications running in the browser, nor do they affect the CRM UI framework, which is used by these applications.

Level of Protection

The URL connection to the back-end system is base64 encoded. The BSP technology ensures base64 encoding for all form parameters in the URL. However, this mechanism is not used within the CRM UI framework. The CRM UI framework does not prevent you from using any sort of security technique. You can also safeguard the data in the URL using either:

- SSL for HTTP

- Direct server communication using HTTP POST

Data Storage Security

Stored Data

Table 386

Data	Storage Location	Stored When	Access Type
Customizing	SAP NetWeaver AS database	Post installation	Read/write/change/delete Only by users with CRM Customizing authorizations
Application data	SAP NetWeaver AS database	User logon/request	Read/write/change/delete
Atom feed	No data is stored by CRM feeds. Note The feed reader can store user credentials. SAP does not have any control over third-party readers.		

The CRM UI framework supports or requires a Web browser as its user interface. The data is stored on the CRM server.

All data stored in the CRM system is protected by the CRM back end. Customizing data can be accessed only by users with CRM Customizing authorizations. This data is accessed by the system administrator during system configuration. Application data is protected by authorization objects. Roles define the authorizations. Users assigned to a role inherit authorizations from that role.

Tracing and Log Files

The following information is traced in the SAP NetWeaver AS cache:

- Messages exchanged between a communication management software (CMS) and the CRM server
- Messages exchanged between ABAP sessions

By default, tracing is switched off. To turn on the trace and change the trace level, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Administration of the Internet Communication Manager*.

Other Security-Related Information

JavaScript

The CRM UI framework uses JavaScript and AJAX to render the UI in the browser, and to handle user interactivity as well. Precautions have been taken against cross-site scripting (CSS) and other related types of attacks.

ActiveX

Table 387

Name	Used In
Microsoft.XMLHTTP	AJAX, e-mail integration (Microsoft Excel, Notes)
Msxml2.XMLHTTP	New version of Microsoft.XMLHTTP
Word.Application	Displaying of data in a Microsoft Word document

Name	Used In
Excel.Application	Displaying of data in a Microsoft Excel spreadsheet
Outlook.Application	Microsoft Outlook integration: ● Exchange of e-mails from Microsoft Outlook to SAP CRM and the other way around ● Address lookup in Microsoft Outlook
Lotus.NotesSession	Lotus Notes integration: ● Exchange of e-mails from Lotus Notes to SAP CRM and the other way around ● Address lookup in Lotus Notes

Required Settings in Microsoft Internet Explorer:

- Active scripting
- Run ActiveX controls and plug-ins
- Initialize and script ActiveX controls not marked as safe (XMLHTTP libraries just need: *Script ActiveX controls marked safe for scripting*)

Cookies

SAP CRM does not use its own session or persistent cookies.

Additional Information

For more information, see the following documents:

- *Enterprise Search Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nwes › *<Choose relevant release>* › *Security Information* › *Security Guide*
- *SAP NetWeaver Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide*
- *Search and Classification (TREX) Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units*
- *Configuration of TREX Security Settings* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View*: Search for *Configuration of TREX Security Settings*.

8.5 Calendar (ActiveX) Control

The activity management and activity scheduling applications use calendar control for the user interface (UI). In this case, the calendar control is an ActiveX control that needs to be installed on each client system together with the activity applications. The ActiveX control does not need any additional libraries other than those present in the installation package.

As in the case of any ActiveX control, the control can only run on Microsoft Windows operating systems and on browsers that support ActiveX. The administrator should provide users with the rights needed to run ActiveX controls.

User Administration and Authentication

The calendar ActiveX control is used by the calendar controller for the UI framework.

Authorizations

The possible scenarios for the installation and use of the calendar ActiveX in the calendar application are the following:

- Installation using automatic download and automatic registration of ActiveX control

  The ActiveX control in a CAB file is signed by SAP. This CAB file is uploaded to the Multipurpose Internet Mail Extensions (MIME) repository of the server. Once you start the calendar application, the ActiveX control is downloaded and installed automatically.
- Installation using an installer

  A Microsoft Windows installer (`*.msi`) is available for the ActiveX control. The administrator can either use this installer to install the control on each individual PC or use a deployment tool like Microsoft Systems Management Services (SMS) for remotely deploying the control. If the ActiveX control is preinstalled, the application uses the installed version of the control without triggering the automatic download.
- No authorization to run ActiveX control

  If you do not use the ActiveX control, users cannot view the calendar in the calendar application. In this case, users should contact the network administrator to obtain the required rights.

  > ➡ Recommendation
  >
  > We recommend that you install the calendar ActiveX control using an installer.

The following security-relevant information should be considered in the context of ActiveX technology and JavaScript code used for rendering the calendar:

- Microsoft ActiveX technology is used for rendering the calendar. The ActiveX control needs to be registered before running the applications that use calendar control. For the case where installation happens using an automatic download, the user of the application requires power user rights to enable automatic registry entry creation.
- The automatic download of ActiveX control and execution of the JavaScript code used for calendar rendering might require changes in Microsoft Internet Explorer (IE) security settings. The Microsoft IE security settings should be set to *Medium* during the download process. The user verifies that the options *Download Signed ActiveX controls* and *Run ActiveX controls and Plug-ins* are enabled in the Microsoft IE security settings before the download process starts. If these options are not already enabled, the user must enable them.

Once downloaded and registered, the calendar application uses this control without causing any further downloads. Only when a new version of the control is available on the server is the download and registration of the new control initiated. The requirements listed above are necessary for this process.

8.6 Access Control Engine

The access control engine (ACE) is an additional authorization concept that exists in parallel to the standard SAP authorization concept.

ACE provides a framework that you can use to control user access to individual business objects and the usage of those business objects. This means that you can define which users see which business objects, and whether those users have the authorization to read, edit, or delete those business objects. ACE supports most business objects that are used in SAP Customer Relationship Management (SAP CRM). For a complete list of supported business objects, see Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *Access Control Engine* › *ACE-Enabled Objects* ◀.

You can set up and configure ACE in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* › *Access Control Engine* ◀. To prevent ACE authorization data from being updated at runtime for changed or created objects when ACE is not in use, use the Customizing activity *Maintain General Parameters* to deactivate ACE as needed.

Why Is Security Necessary?

ACE manages object authorizations for users, which therefore need to be protected. Manipulation of authorization data can lead to the assignment of incorrect authorizations. This means that users may have authorizations that they should not have.

User Administration and Authentication

You use ACE user groups to assign users to ACE rights. Those user groups can contain reference users, roles, or collective roles. User groups can also contain other user groups.

⚠ Caution

Changes to roles, reference users, and ACE user groups affect the authorization data of ACE.

After reactivating a corresponding right or refreshing the user context by using *ACE Update Tool* (transaction `ACE_UPDATE`), ACE runtime tables reflect the changes made.

ℹ Note

The user context refreshes automatically after 16 hours (customizable value).

To maintain user groups, you can use *ACE Design Report* (transaction `ACE_DESIGN`).

To check the authorization data, you can use *ACE Runtime Report* (transaction `ACE_RUNTIME`).

User Data Synchronization

ACE references the *User Maintenance* (`SU01`) transaction. If you want to delete a user created using transaction `SU01`, there is a dependency that requires specific steps.

⚠ Caution

Before deleting a user created using transaction `SU01`, review the following section.

Deleting Users

Before you delete the user, delete it from all user groups in which it has `Child-Type = U` and refresh these user groups.

To do so, make the settings in Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Create Rights and Update User- and Object Context*.

Authorizations

To maintain the ACE design time tables using *Maintain Table Views* (transaction SM30) or *View Cluster Maintenance* (transaction SM34), an ACE administrator needs to be assigned to authorization object S_TABU_DIS:

Table 388

Authorization Object	Field	Value	Description
S_TABU_DIS	ACTVT	2	Change authorization for table maintenance (using standard tools, such as SM30)

The following important ACE runtime tables are secured by authorization object S_TABU_DIS:

- CRM_ACE_ST_ACC
- CRM_ACE_OTYPES
- CRM_ACE_CUSTOM
- CRM_ACE_RIGHTS
- CRM_ACE_RULES
- CRM_ACE_U_GRP
- CRM_ACE_U_GRPS
- CRM_ACE_WP
- CRM_ACE_WP_OTS

Recommendation

Do not assign S_TABU_DIS authorization to users for these runtime tables in a productive system.

In addition to authorization object S_TABU_DIS, an ACE administrator needs special authorizations to start and use the *ACE Design Report* (transaction ACE_RUNTIME), *ACE Update Tool* (transaction ACE_UPDATE), and *ACE Activation Tool* (transaction ACE_ACTIVATION), and to make changes using these tools:

Table 389

Authorization Object	Field	Value	Description
CRM_ACE_MD	ACTVT	16 (Execute)	Authorization to start the following ACE transactions: • ACE_ACTIVATION • ACE_DESIGN • ACE_UPDATE • ACE_RUNTIME
CRM_ACE_MD	ACTVT	63 (Activate)	Authorization to activate ACE rights and user groups

Authorization Object	Field	Value	Description
CRM_ACE_MD	ACTVT	66 (Refresh)	Authorization to refresh ACE rights, user contexts, and object contexts
CRM_ACE_MD	ACTVT	H1 (Deactivate)	Authorization to deactivate ACE rights and user groups

⚠ Caution

Users who have these authorization objects assigned to them have access to all ACE-relevant runtime and design data.

Data Storage Security

ACE saves runtime and design data, such as user context cache, in the database of the SAP system, as well as temporarily on one or more application servers. Access to the data on the database is restricted by authorization objects.

The runtime data is written during the activation of rights and after the creation or changes of ACE-relevant objects by background processes. You can see the status of a rights activation by checking the *Monitoring* tab in the *ACE Activation Tool* (transaction ACE_ACTIVATION).

⚠ Caution

Failed objects of a rights activation indicate incorrect authorization data. To correct them, use the *Send to Update Tool* button.

During runtime, when authorization queries are made to ACE, the system mainly reads the calculated data. You can check the runtime data by using *ACE Design Report* (transaction ACE_RUNTIME).

The runtime data is stored in a set of three database tables. For each ACE-relevant superordinate object type such a set of tables exists. The following naming convention applies to the tables:

- CRM_ACE2_*_GRP
- CRM_ACE2_*_ACL
- CRM_ACE2_*_UCT

The asterisk (*) stands for the identifier of the superordinate object type and can contain up to three characters.

Security-Relevant Logging and Tracing

You can switch on table logging to log data that is deleted, added, or changed in the ACE tables. For each table, the audit mechanism logs the user names and the changes that the user made.

Table logging is enabled for the following database tables in the standard system:

Table 390

Technical Name	Description
CRM_ACE_ACTTYP	Definition of actor type
CRM_ACE_CUSTOM	Customizing
CRM_ACE_OTYPES	Object types

Technical Name	Description
CRM_ACE_RIGHTS	Rights
CRM_ACE_RULES	Rules
CRM_ACE_ST_ACC	Assignment of table names to super types

If necessary, we recommend that you also activate logging for the following tables:

Table 391

Technical Name	Description
CRM_ACE_RIG_RT	Activated rights
CRM_ACE_UGR_RT	Activated user groups
CRM_ACE_AFO_CL	Determination of actors for the object
CRM_ACE_AFU_CL	Determination of actors for the user
CRM_ACE_OBF_CL	Determination of objects using a filter
CRM_ACE_ANGRP	Action groups
CRM_ACE_ANGRPS	Assignment of actions to action groups
CRM_ACE_U_GRP	User groups
CRM_ACE_U_GRPS	Assignment of users, roles, or groups to user groups
CRM_ACE_WP	ACE work package definition
CRM_ACE_WP_RT	ACE work package runtime data
CRM_ACE_TRACE	ACE object trace

You can activate and deactivate the tables in the ABAP Dictionary. You can view the log results in the table history using the transaction *Analysis of Logged Customizing Objects and Tables* (SCU3).

For more information about logging table data changes, see SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform ❯ *<Choose relevant release>* ❯ *Security Information* ❯ *Security Guide* ❯ *Security Aspects for Lifecycle Management* ❯ *Auditing and Logging* ◀.

ACE Restrictive Mode

In the standard system, ACE always grants users access to requested objects in the following cases:

- ACE is inactive
- Requested action unknown
- Requested object type unknown
- User is not active in ACE

By setting ACE in restrictive mode, you can invert this behavior. Then ACE only grants access to objects if the user has this authorization given by an activated ACE right.

To activate the restrictive mode, you need to set the parameter RESTRICTIVE_MODE to value **x** in Customizing for *Customer Relationship Management* under ▶ *Basic Functions* ❯ *Access Control Engine* ❯ *Maintain General Parameters* ◀.

8.7 Knowledge Management

The Knowledge Management (KM) component delivers functions and services for managing unstructured or partially structured content. It enables the user to save and find documents in different types of repositories, and allows the user to find and access information using advanced information finding and document classification methods. It supports Web authoring and publishing and includes form-based publishing of standard content. The KM component offers generic services, for example, for informing users about changed content and for introducing approval processes into the publishing process.

Related Security Guides

Table 392

Application	Guide
Content management	*Search and Classification (TREX) Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Search and Classification (TREX) Security Guide*

Why Is Security Necessary?

Security is necessary to protect internal documents from misuse due to external access or access from other departments. If documents are not protected, sensitive data may become public knowledge and harm your enterprise.

Documents may also contain viruses that can damage your entire network if they are not discovered and eliminated in time. Some viruses only block the flow of data by automatically sending e-mails. Other viruses wantonly delete entire datasets, and the user can do nothing to prevent it.

User Administration and Authentication

Integration with the Single Sign-On Environment

KM works in a single sign-on (SSO) environment.

Authorizations

Authorizations for the Info Center Directory Structure

You have the option to restrict access to the info center according to individual user groups. This is particularly important, for example, if you store business-related evaluations that your employees may not see in the info center, or store data that must not be seen by customers or partners because of data protection restrictions.

> Recommendation
>
> We recommend that you give your users only the most necessary authorizations to keep the risk of unauthorized access to a minimum. For more information, see SAP Solution Manager.

Activating the CRM News Scenario

If you are using the SAP CRM news scenario, make sure that the CRM namespace filter is configured and active in your system. If not, unauthorized users may be able to read news to which they should not have access.

For more information about configuring the news filters, see SAP Solution Manager under *Creating and Adjusting News Filter*.

Furthermore, you can restrict access to news channels (folders in the `sapcrmnews` repository) by setting KM authorizations.

For more information about setting authorizations, see SAP Solution Manager under *Setting Permissions*.

Publish CRM Documents Using a WebDAV Handler

SAP CRM offers the option of publishing documents that are attached to CRM business objects by using a WebDAV server. For more information, see SAP Solution Manager. The documents can be integrated into KM as a WebDAV repository, so they can be indexed and found with a search (TREX).

The corresponding SAP NetWeaver Application Server (SAP NetWeaver AS) service (`/default_host/sap/crm/crm_prt_km_dav`) is deactivated by default, like all other services, so no documents can reach the outside world. The HTTP service represents the interface of the Web-Based Distributed Authoring and Versioning (WebDAV) service to the outside world. If you do not use an anonymous logon, make sure that you have performed the steps described in SAP Note 686776.

For more information, see

- Authorizations [page 25]
- *Maintaining Authorizations for WebDAV Hierarchies* in SAP Solution Manager.

The standard SAP NetWeaver AS security model holds for activating the service. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Security Guides for SAP NetWeaver Functional Units* > *Security Guides for the AS ABAP*.

Security Aspects of Data Flow and Processes

The figure below shows an overview of the data flow for Knowledge Management

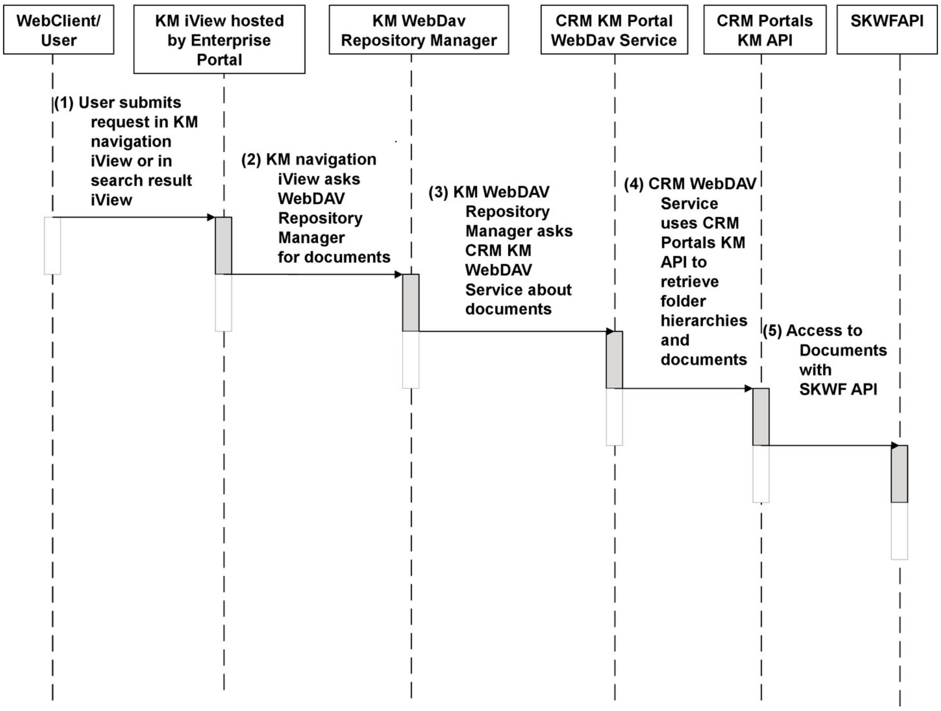

WebClient/ User
KM iView hosted by Enterprise Portal
KM WebDav Repository Manager
CRM KM Portal WebDav Service
CRM Portals KM API
SKWFAPI
(1) User submits request in KM navigation iView or in search result iView
(2) KM navigation iView asks WebDAV Repository Manager for documents
(3) KM WebDAV Repository Manager asks CRM KM WebDAV Service about documents
(4) CRM WebDAV Service uses CRM Portals KM API to retrieve folder hierarchies and documents
(5) Access to Documents with SKWF API

Figure 30: Overview of Process Steps for Knowledge Management

Table 393

Step	Description	Security Measure
1	User submits request in KM navigation iView or in search result iView.	Restrict access to enterprise portal and iViews to known users or user groups
2	KM navigation iView asks WebDav Repository Manager for documents	When creating a WebDAV repository on the KM side, you might enter authentication data into the system landscape entry of the WebDAV repository manager. This gives anyone who is able to log on access to the CRM documents. This should be avoided. To prevent this from happening, choose the landscape option *Same User Domain*. The user then sees only those documents that are seen in SAP CRM. For more information, see SAP Note 686776
3	KM WebDAV Repository Manager asks CRM KM WebDAV service about documents	You might enter authentication data or an alias into the service. This gives everyone access so it should be avoided except perhaps for short tests.
4	CRM WebDAV Service uses CRM Portals KM API to retrieve folder hierarchies and documents	For information on maintaining the authorization object `CRM_DOCS_H`, see SAP Solution Manager.
5	Access to documents with SKWF API	not applicable

8.8 Interactive Reporting

Interactive reporting in SAP Customer Relationship Management (SAP CRM) enables reporting on CRM business data without a separate SAP NetWeaver Business Warehouse (SAP NetWeaver BW). The solution is based on the SAP NetWeaver BW that comes with SAP CRM and can be used to run CRM interactive reports on the same machine.

This section provides security-relevant information for interactive reporting in SAP CRM.

Security Aspects of Data, Data Flow, and Processes

The following criteria determine which business data a user can access in interactive reporting:

- Organizational position of the user, whether the user is a manager or not
- Responsibility of the user with respect to the business data

Example

The interactive reports of sales representatives include only the business data for which they are responsible, such as the opportunities they have created. In contrast, the interactive reports of sales managers include all business data for which the sales representatives of their teams are responsible.

The figure below shows an overview of the data flow for interactive reporting:

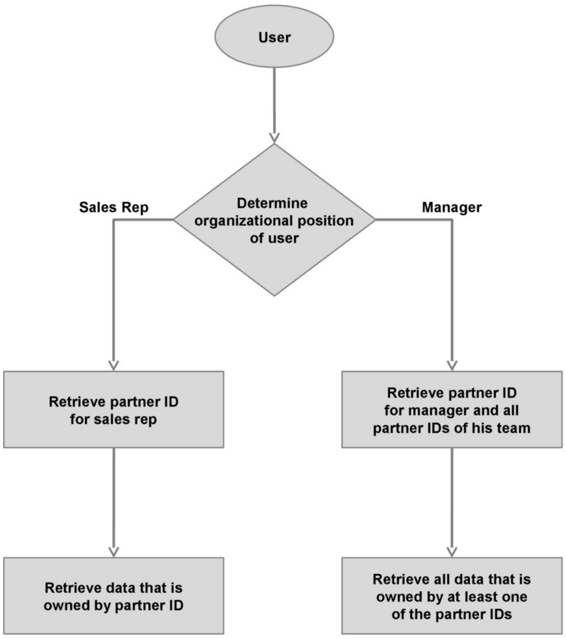

User
Determine organizational position of user
Sales Rep
Manager
Retrieve partner ID for sales rep
Retrieve partner ID for manager and all partner IDs of his team
Retrieve data that is owned by partner ID
Retrieve all data that is owned by at least one of the partner IDs

Figure 31: Dataflow Interactive Reporting

User Management

User authorizations in interactive reporting are determined by assigning PFCG roles to a user as follows:

Table 394

PFCG Role	User Authorization
CRM Interactive Reporting User Role (SAP_CRM_OR_USER)	Running interactive reporting
CRM Interactive Reporting Administrator Role (SAP_CRM_OR_ADMIN)	• Activating interactive reporting (report areas and/or CRM reports) • Changing interactive reports delivered by SAP
CRM Analytics Professional Role (SAP_CRM_UIU_ANALTYICSPRO_UI)	Creating and publishing custom interactive reports

Assignment of Report Areas

You determine the range of fields that can be used for interactive reports by assigning specific report areas to the user. You do this in Customizing for *Customer Relationship Management* under *CRM Analytics* > *Map Report Areas to Business Role*.

Custom Enhancement of Interactive Reporting

For custom enhancements of interactive reports (custom fields) you need an RFC connection for user `ALEREMOTE`.

> **Note**
>
> You can define the RFC connection in *Customer Relationship Management* under ▶ *CRM Middleware and Related Components* › *Communication Setup* › *Define RFC Destinations* ◀.

In *User Maintenance* (transaction `SU01`) assign the following profiles to user `ALEREMOTE`:

- *Business Information Warehouse, RFC-User Extraction* (`S_BI-WX_RFC`)
- *Business Information Warehouse, RFC user in the Warehouse* (`S_BI-WHM_RFC`)

Additional Information

For custom enhancements of interactive reporting, note the following:

- Internal system processes (background processing) or system-related processes require a user of type *System*.
- Dialog logon (using SAP GUI) is not enabled.
- Users are excluded from the general settings for password validity if they are specified as follows:
  - User group *Super*
  - User type *System* or *Service*.

  System administrators can change the password in *User Maintenance* choosing ▶ *Goto* › *Change Password* ◀.
- Multiple logons are allowed.

Authorizations

The following security-relevant authorization objects are used by interactive reporting:

Table 395

Authorization Object	Field	Value		Description
`CRM_OR_ADM`	`ACTVT`	02	Change	Used in role *CRM Interactive Reporting Administrator Role* (`SAP_CRM_OR_ADMIN`)
		03	Display	
		21	Transport	
		23	Maintain	
		63	Activate	
		71	Analyze	
	`OR_OBJTYPE`	IT	Report Area	Type of interactive reporting object
		RP	Report	
		VW	View	
`CRM_ANA_PR`	`IS_ANAPRO`	X <blank>		*X* indicates PFCG role *CRM Analytics Professional Role*

Authorization Object	Field	Value	Description
			(SAP_CRM_UIU_ANALTYICSPRO_UI) is assigned to the user

Communication Destinations

The following communication destinations are used by interactive reporting:

Table 396

Destination	Delivered	Type	User, Authorizations	Description
Connections to CRM clients	No	Trusted RFC, ABAP	In *Configuration of RFC Connections* (transaction SM59) define the following: ● On tab *Logon & Security* select *Current User* ● For *Trust Relationship* select *Yes* (authorization object S_RFCACL)	RFC connections to the CRM source clients enabling login without login screen
Connection to BW client	No	RFC, ABAP	User ALEREMOTE	RFC connection to the BW client

9 Component-Specific Guidelines: Industries

9.1 SAP Leasing

The SAP Leasing application provides a complete end-to-end solution for all companies that lease out assets. It supports all steps in the financing contract lifecycle, from a financing opportunity for a lease or a loan to an offer, through to mid-lease changes, and resulting in end-of-lease options.

Furthermore, a remarketing process is combined with the solution for each lease object (for example, leased car). The solution also addresses all expected international requirements, including multilanguage and multicurrency capabilities, parallel valuation according to multiple international accounting standards, and local accounting rules. SAP Leasing is the only solution that combines integrated, enterprise-wide financial functions with world-class Customer Relationship Management capabilities. As such, the front office for sales and service related processes (SAP CRM) is seamlessly integrated with the back office (SAP ERP) for all accounting processes.

User Management and Authentication

User Management

Table 397

Tool	Description
User and role administration with SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP): *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	For more information, see User Administration and Authentication [page 18].

User Types

Table 398

System	User	Delivered?	Type	Default Password	Description
SAP CRM	End user	No	Dialog user	No	Mandatory user who can access sales, presales, and billing transactions. Created by an SAP CRM system administrator.
			System user	No	Mandatory user who can process background jobs. Created by an SAP CRM system administrator.
					Mandatory user for data exchange between SAP CRM and SAP ERP. Created by an SAP CRM system administrator.

System	User	Delivered?	Type	Default Password	Description
SAP ERP	End user	No	System user	No	Mandatory user for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, the user can be an individual user or a system RFC user. Created by an SAP ERP system administrator.
					Mandatory user for data exchange between SAP Supplier Relationship Management (SAP SRM) and SAP ERP. Depending on the RFC destination, the user can be an individual user or a system RFC user. Created by an SAP ERP system administrator.
SAP SRM	End user	No	Dialog user	N/A	Mandatory user who can access purchase order request.
			System user	N/A	Mandatory user for data exchange between CRM and ERP.

Authorizations

Leasing is a cross-system scenario. Therefore, the transactions linked in the work center of a business profile (WebClient UI) involve CRM transactions and back end transactions, such as the Lease Accounting Engine (SAP ERP), or extracting BI reports with SAP Business Intelligence. In principle, the standard SAP authorization concept is sufficient for SAP Leasing.

If the SAP standard authorization concept is not sufficient, we recommend that you use customer-specific enhancements, such as the access control engine (ACE).

Authorization for Sensitive Data (SAP CRM)

The security of sensitive data must be ensured. This is the case, for example, when company employees are also business partners who are leasing a car.

This authorization issue could be solved in the following way: Leasing quotations and contracts for employees must be created using specific business transaction types and item types within the CRM business transaction. To handle leases for employees, we recommend that you use customer-defined sales organizations. In addition, the user profile of employees should be restricted for at least the following authorization objects:

Table 399

Authorization Object	Description
CRM_ORD_PR CRM Order	Business Transaction Type
CRM_ORD_OE CRM Order	Allowed Organizational Units
B_BUPA_GRP	Business Partner – Authorization Groups

To control the maintenance of specific business partner data in financial service (FS) accounts on the WebClient UI, the user profiles in the authorization object Business Partner: Authorization Group (`B_BUPA_GRP`) should be restricted.

Furthermore, any changes to leasing documents are dependent on the status of the document and on the hierarchy level of the user. We recommend that you define a customer-specific structure for changes to leasing documents in Customizing for *Customer Relationship Management* under□ ▶ *Financial Services* ▸ *Leasing* ▸ *Readiness for Input of Transaction Fields* ◀.

Authorization for Worklists (SAP ERP)

In the area contract accounts receivable and payable (FI-CA) the authorization objects *Authorization for Worklist* (`/LSIERP/WL` and `/LSIERP/WI`) are used to create a worklist during the dunning run.

Table 400

Authorization Object	Description
`/LSIERP/WL`	Includes the permitted activities create or generate, change, and display, and the *Activity* field. A user can be authorized to create, change, or display a worklist.
`/LSIERP/WI`	Includes the permitted activities create or generate, change, and display, and the *Activity* and *Company Code* fields. A user can be authorized to create, change, or display a worklist item for each company code.

To control the maintenance of specific business partner data in financial service (FS) accounts on the WebClient UI, the user profiles in the authorization object *Business Partner: Authorization Group* (`B_BUPA_GRP`) should be restricted.

The WebClient UI for FS accounts is based on the WebClient UI for CRM business partners and therefore offers the same authorization settings; in particular the authorizations for the access control engine (ACE) are checked.

Other Security-Relevant Information

All recommendations concerning SAP CRM are also relevant for the SAP Leasing scenario. The recommendations concerning connected back-end systems, such as SAP ERP and SAP Supplier Relationship Management (SAP SRM), are also relevant. For more information, see the following security guides:

Table 401

Application	Guide
SAP ERP	*SAP ERP Security Guide* on SAP Service Marketplace at service.sap.com/securityguide
SAP NetWeaver Exchange Infrastructure	*SAP NetWeaver Exchange Infrastructure Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform ▸ *<Choose relevant release>* ▸ *Application Help* ▸ *Function-Oriented View* ◀: Search for *SAP NetWeaver Exchange Infrastructure Security Guide*
SAP SRM	*SAP SRM Security Guide* on SAP Service Marketplace at service.sap.com/securityguide

9.2 SAP Account Origination

The SAP Account Origination application for financial services is an integrated customer-oriented software solution, linking the front office (WebClient UI) to the back office (core processing applications for banking or insurance).

This business scenario covers a variety of processing application flows in the financial services industry. Sample content is provided for the most-requested scenario: origination of loans.

The business scenario starts with a customer applying for a financial services product that is provided by a financial services institute, and ends when the contract is signed by both parties. The scenario includes the analysis of customer data and requirements, calculation and creation of quotations for the customer, underwriting, risk assessment and validation, as well as parts of the closing and funding process.

In SAP Solution Manager, you can find the description of this scenario under *SAP for Banking* > *Scenarios* > *Account Origination*.

Technical System Landscape

The following software components are required or optional, as indicated below, for the technical implementation of the account origination scenario:

Table 402

Component	Required or Optional	Comment
SAP CRM (Web application server (AS))	Required	Within SAP CRM, CRM AS ABAP is needed for the account origination scenario.
SAP NetWeaver Process Integration (SAP NetWeaver PI)	Required	You require SAP NetWeaver PI as middleware for connecting the software components. SAP NetWeaver PI enables synchronous as well as asynchronous data exchange between the business systems to which it is connected.
Contract System	Required	The account origination scenario requires at least one contract system for the operational management of the contracts. Depending on the type of contract (such as loan contracts, collateral agreements, or insurance contracts) additional functions are required (such as rating and calculation).

Note

You can use SAP components as well as components from other manufacturers as contract and support systems.

User Administration and Authentication

User Management

User management is described in the following table:

Table 403

Tool	Description
User and role administration with SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP): User Maintenance (SU01) transaction and the profile generator (PFCG) transaction	For more information, see User Administration and Authentication.

User Types

User types are described in the following table:

Table 404

System	User	Delivered	Type	Default Password	Description
SAP CRM	End User	No	Dialog User	No	Mandatory user who can access sales and presales transactions. Created by an SAP CRM system administrator.
SAP CRM	PI User	No	System User	No	Mandatory user for data exchange between CRM and PI System. Created by an SAP CRM system administrator.

Authorizations

Account origination is a cross-system scenario. As such, the linked transactions in the work center (WebClient UI) relate to CRM transactions and also to the transactions in the back-end systems. The standard SAP authorization concept is usually sufficient for account origination.

The following standard role is delivered for account origination:

Table 405

Role	Description
`SAP_CRM_UIU_FSAO_MANAGER`	CRM UIU FS Account Origination Manager

Let's consider a typical user scenario and examine an example of a specific security issue that can arise.

A finance company also provides loans for employees. The origination process includes a rating request, the results of which are saved in the business partner file and the quotation. This data must not be visible for other employees because it contains sensitive data, such as collaterals, lending values, loans, and so on. The security of this sensitive data must be ensured. The authorization problem mentioned above could be resolved using the following approach.

Employee loans, and indeed all financial service quotations for employees, must be created using specific business transaction types and item types within the CRM business transaction. SAP recommends using a specific user-defined sales organization to handle employee loans. Furthermore, the user profile of employees in the following authorization objects should be restricted:

Table 406

Authorization Object	Description
CRM_ORD_PR CRM Order	Business Transaction Type
CRM_ORD_OE CRM Order	Allowed Organizational Units

To control the maintenance of specific business partner data in financial services (FS) accounts in the WebClient UI, the user profiles in the following authorization object must be restricted:

Table 407

Authorization Object	Description
B_BUPA_GRP	Business Partner: Authorization Group

The WebClient UI for FS accounts in SAP CRM is based on the WebClient UI for CRM business partners, and therefore offers the same authorization settings; in particular, the system checks the authorizations for the Access Control Engine (ACE).

Other Security-Relevant Information

All recommendations concerning SAP CRM are also relevant for the SAP Account Origination. For more information, see the following security guide:

Table 408

Application	Guide
SAP NetWeaver Process Integration	*SAP NetWeaver Process Integration Security Guide* in SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform ❯ *<Choose relevant release>* ❯ *Application Help* ❯ *Function-Oriented View* ◀: Search for *SAP NetWeaver Process Integration Security Guide*

9.3 SAP Social Services Management for Public Sector

SAP Social Services Management for Public Sector is a package that provides a set of integrated functions and specific service transactions to support the fully electronic processing of social benefit applications. The CRM processes are closely linked to an ERP system that performs the complex calculation algorithms required for social service processes.

The central feature of SAP Social Services Management for Public Sector is the configuration of automatic application processing. Rule-based checks performed by the system are used to automatically analyze and process the applicant data submitted. After replication to the ERP system, several calculation steps are executed, and the billing and accounting are performed for the determined amount. As a result, the case worker has fewer tasks to perform, and can focus on the most important ones. If required, you can even support fully automated application processing.

Related Security Guides

All recommendations concerning SAP Customer Relationship Management (SAP CRM) are also relevant for SAP Social Services Management for Public Sector.

For more information about additional functions in SAP ERP for SAP Public Sector Collection and Disbursement, observe the following security requirements in the SAP ERP security guide:

- *SAP Public Sector Collection and Disbursement (SAP PSCD) Security Guide.*
- Security requirements for the use of payment cards under *Payment Card Security*.

For a complete list of the available SAP security guides, see SAP Service Marketplace at service.sap.com/securityguide.

Authorizations

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

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

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). The new SAP Social Services Management for Public Sector business objects social application, social service plan and social deduction plans and Case Management for Public Sector, have been adapted for the use of the ACE. The standard role SAP_FMCA_CA_ALL_EHP5 can be used to cover the required authorizations needed for the FI-CA transactions in the ERP system. This role should only be assigned to the (SAP ERP) users for the caseworkers, if you are using PSCD and FI-CA functions (such as FCC). If this is not the case, the standard SAP ERP caseworker role should be sufficient.

Standard Roles

The following table shows the standard roles that are used by SAP Social Services Management for Public Sector:

Table 409

Role	Description
SAP_CRM_UIU_CASEWORKER (CRM side)	The role includes all authorization objects that a case worker needs when working with the WebClient UI (using business role CASEWORKER). This role itself cannot be used, it is simply a template. Instead, customers have to copy and customize the role.
SAP_PSSC_ERP_CASEWORKER (ERP side)	This role is the counterpart of the CRM role SAP_CRM_UIU_CASEWORKER. Each case worker in CRM needs this role to be assigned to their user in the ERP system to execute the ERP-related tasks.

Role	Description
SAP_PSSC_ERP_FINANCIAL_CLERK (ERP side)	This role is for financial clerks or FI-CA account managers in the social service solution. It contains the main transactions that are necessary to start the ERP mass run for billing and net calculation, and several other required transactions.
SAP_CRM_4S_ADMINISTRATOR	This role is designed to be used by administrators of the Social Services solution in the CRM System. It contains (technical) programs and RFC function modules that are needed for the Application Enhancement Tool (AET).
SAP_PSSC_ERP_ADMINISTRATOR	This role is designed to be used by administrators of the Social Services solution in the ERP System. It contains (technical) programs.

After you have copied the role SAP_CRM_UIU_CASEWORKER to your own role or profile in the profile generator (PFCG) transaction, deactivate the authorization object S_SERVICE (S_SERVICE contains outbound plugs for navigation; this authorization object cannot be generated). All necessary authority checks are performed using the authorization object UIU_COMP, which is found in the standard role SAP_CRM_UIU_CASEWORKER. Note that in the authority object CRM_VIEW (*Authorization Object CRM Order - Request Category View*), you must maintain the name of the request category that you want to use for the SAP_CRM_UIU_CASEWORKER role.

Authorization Objects

The following authorization objects are available for SAP Social Services Management for Public Sector in SAP CRM:

Table 410

Authorization Object	Field	Value	Description
CRM_SOA	ACTVT	45 (Allow)	CRM business transaction *Social Application.* This authorization object is used when handling a social application and a payment request..
CRM_SSP	ACTVT	45 (Allow)	CRM business transaction *Social Service Plan*. This authorization object is used when handling a social service plan.
CRM_SDP	ACTVT	45 (Allow)	CRM business transaction *Social Deduction Plan*. This authorization object is used when handling a social deduction plan.
CRM_DBA	ACTVT	45 (Allow)	CRM business transaction *Decision Basis*. This authorization object is used when handling a decision basis.
CRM_SOC_AP	PR_TYPE	<Business transaction type>	Approval of Social Application/Social Service Plan.

Authorization Object	Field	Value	Description
	AP_LEVEL	The value that is needed for sufficient approval rights depends on the implementation of the Business Add-In (BAdI) CRM_PS_APPROVAL (method DETERMINE_DOCUMENT_LEVEL). You must assign the value that is requested in the BAdI to a user here, to allow approval of a business transaction. Note that if you have not implemented the BAdI method DETERMINE_DOCUMENT_LEVEL, approval is also possible with value 000 or *.	This authorization object is used during the approval process for a Social Service business transaction, such as a social application, a social service plan, a social deduction plan and a payment request.
CRM_4S_CPE	ACTVT	16 (Execute a change process)	Authorization check for social service plan change processes. This authorization object is used during the execution of a change process with the change process engine (CPE).
	CHNGPROC	<Change process>	
	CP_EXEC_PR	<Business transaction of change process>	
CRM_4S_ADM	ACTVT	16 (Execute)	Authorization object for SAP CRM administrators.
	PROGRAM	<Program name> If the authorization check takes place within and for a program, the program name is checked here.	
CRM_4S_AET	ACTVT	03 (Display)	Authorization to display AET relevant DDIC information. Only relevant for adminitrators setting up the AET extensions in SAP ERP.

In addition to these special authorization objects, SAP Social Services Management for Public Sector uses the standard authorization objects for all reused functions, such as CRM business transaction or Case Management.

The following authorization objects are available for SAP Social Services Management for Public Sector in SAP ERP:

Table 411

Authorization Object	Field	Value	Description
F_SC_SXP	ACTVT	01(Create or generate) 02 (Change) 03 (Display)	The F_SC_SXP authorization object checks the authorization for displaying, changing, or creating the following social service business objects: social service plan (SSP), social deduction plan (SDP), gross
	PSSCSXPTYP	Value from table PSSCC_SXP_TYPE	

Authorization Object	Field	Value	Description
			entitlement document (GED), and gross payment document (GPD). The authorization for these business objects is based on the type of the corresponding social service plan or social deduction plan, that is, the SXP type.

`F_SC_NCD`	`ACTVT`	01(Create or generate)
		02(Change)
		03(Display) 05(Lock)
		06(Delete)
			For the object types `SSP, SDP, GED`, and `GPD`, the authorization object `F_SC_SXP` is essential, because the access of case workers to certain SSPs and SDPs depends on their SXP type, and likewise - based on that - the access to GEDs and GPDs. Net calculation documents (NCDs) do not have a field for the SXP type. Therefore, the `F_SC_SXP` authorization object does not make sense here. In this case, it is sufficient to check the general access to the payment family itself, which is possible using the `F_SC_NCD` authorization object.

	`PSSCPAYFAM`	Value from DDIC element `PSSC_PAYMENT_FAMILY`	
`F_SC_ADM`	`ACTVT`	`16 (Execute)`	Authorization object for SAP ERP administrators.
	`PROGRAM`	<Program name> If the authorization check takes place within and for a program, the program name is checked here.	

Other Security-Relevant Information

Social Services Eventing

Social services eventing (SSE) is implemented using remote function calls (RFCs). RFCs allow customers to create different authorizations for users who have triggered an event and for RFC users who are executing this event. Both users can have different sets of authorizations. Therefore, it is not necessary to grant users who are triggering an event all the rights that are necessary to execute this event. The rights necessary to execute the event need to be granted only to the RFC users who are assigned to the RFC destination.

The assignment of an RFC destination to an SSE event can be done in Customizing for *Customer Relationship Management* under ▶ *Industry-Specific Solutions* › *Public Sector* › *Social Services* › *Common Functions* › *Social Services Eventing* › *Process SSE Customer Control Parameters* ◀.

Here, an RFC destination can be specified in the *Parameter Value* field using *Parameter ID* `Destination`.

Usage of BRFplus in Social Services

In SAP CRM and SAP ERP, the Business Rule Framework plus (BRFplus) rule engine can be used to execute customer-defined rules (for example to determine which payment items a citizen can claim). If system administrators need to create new customer-defined rules in BRFplus, the role SAP_BC_FDT_ADMINISTRATOR can be used.

Network and Communication Security

Your network infrastructure is essential in protecting your system. Your network needs to support the communication necessary for your business 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, there is no way for intruders to compromise the machines and gain access to the database or files in the back-end system. Additionally, if users are not able to connect to the server local area network (LAN), they cannot exploit well-known bugs and security loopholes in network services on the server machines. The network topology for this scenario 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 this scenario.

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

- *Network and Communication Security*
- *Security Aspects for Connectivity and Interoperability*

Communication Destinations

SAP does not deliver any RFC destinations for the social service scenario. For all RFC calls mentioned below, we recommend using trusted RFCs with the same user in both systems. Grant users the following authorizations:

- In the RFC client system (the calling system, for example SAP CRM):

  S_ICF: This authorization object controls which RFC destinations a user may use.
- In the RFC server system (the called system, for example SAP ERP):
  - S_RFC: Maintain the function groups that contain the RFC function modules that you want to allow a user to call (see below).
  - S_RFCACL: Checked when trusted RFC is used. We recommend that you use the same user in both the calling and the called system. If you follow this recommendation, set the RFC_EQUSER field to Y.

RFC Calls from SAP CRM to SAP ERP

All RFC function modules in the SAP ERP system that are called start with PSSC00_REPL and are all found in the function group PSSC00_REPL. You have to enter this function group in the respective authorization field for S_RFC. These calls are used to manage the synchronization of the master and transactional data that is required for the calculations in SAP ERP. These RFC calls are also used to handle manual steps executed.

Since no RFC destinations are delivered in the standard system, you have to create your own destination to the ERP system. The middleware also needs to have RFC destinations assigned that synchronize order objects, Customizing, and business partner (BP) data between the SAP CRM system and the SAP ERP system.

The following section contains a brief overview of the RFC function modules that are called from the SAP CRM system in the SAP ERP system:

Table 412

Name of Function Module	Description
Collected in the function group PSSC00_REPL and PSSC00_DBA_REPL	
Function Modules at Design Time for Customizing Check Reports	

Name of Function Module	Description
PSSC00_REPL_GET_CUSTOMIZING	Reads social service plan Customizing
PSSC00_DBA_REPL_GET_CUST	Reads decision basis Customizing
PSSC00_REPL_VIEWCLUSTER_CALL	Call complex data object maintenance
PSSC00_REPL_VIEW_IMPL_CALL	Display BRFplus application or BAdI implementation
PSSC00_REPL_VIEW_MAINT_CALL	Navigation to maintenance view
Function Modules at Run Time	
PSSC00_REPL_SSP_GE_CALCULATE	Triggers gross entitlement calculation
PSSC00_REPL_SSP_GP_CALCULATE	Triggers gross payment calculation
PSSC00_REPL_SSP_RR_EXECUTE	Execute reimbursement for SSP chain
PSSC00_REPL_SSP_RR_READ	Read reimbursement
PSSC00_REPL_SXP_BA_CHECK	Before assessment check for SXP
PSSC00_REPL_SXP_COMMIT	Commit work
PSSC00_REPL_SXP_FLUSH_BUFFER	Flush
PSSC00_REPL_SXP_GET_ALL	Reads all data for SXP
PSSC00_REPL_SXP_GET_PAY_INFO	Gets SXP payment info
PSSC00_REPL_SXP_PROXY_UPLD_MW	SXP proxy upload to ERP
PSSC00_DBA_REPL_PROXY_UPLD_MW	Decision basis data proxy upload to ERP
PSSC00_REPL_SXP_ROLLBACK	Rollback
PSSC00_REPL_SXP_SAVE	Save
PSSC00_REPL_SXP_SIMULATE_NET	Executes net calculation and reads the simulation results
PSSC00_REPL_SXP_STATUS_ADJUST	Confirms proxy communication
PSSC00_REPL_PREQ_GET	Gets ERP payment request data
PSSC00_REPL_PREQ_MW	Payment request proxy upload to ERP
PSSC00_REPL_PREQ_MW_CONFIRM	Confirms payment request
PSSC00_REPL_PREQ_OLTP	Creates payment request in buffer
PSSC00_REPL_PREQ_REVERSE	Reverses payment request
PSSC00_REPL_PREQ_SAVE	Saves payment request in the ERP database

RFC calls from SAP ERP to SAP CRM

Use of the application enhancement tool (AET) for table enhancements requires in the SAP ERP RFC function modules to read some (meta) data from the SAP CRM system. All of these AET-related function modules belong to the function group CRM_4S_EEW_CUST. Since no RFC destinations are delivered in the standard system, you have to create your own destinations to the SAP CRM system.

The following section contains a short overview of the RFC function modules that are called from the SAP ERP System to the SAP CRM System:

Table 413

Name of function module	Description
Collected in the function group CRM_4S_EEW_CUST	
CRM_4S_AET_READ_DOMA	Read domain of AET table
CRM_4S_AET_READ_DTEL	Read data element of AET table
CRM_4S_AET_READ_METADATA	Read AET metadata Customizing (RFC)
CRM_4S_AET_READ_TABL	Read transparent table type for AET table
CRM_4S_AET_READ_TTYP	Read table type for AET table
Collected in the function group CRM_PS_DBA_REMOTE_ACCESS	
CRM_PS_DBA_GET_ENTITY_LIST	Returns a list with all active entity type headers
CRM_PS_DBA_GET_ENTITY_TYPE	Read one specific entity type
CRM_PS_DBA_GET_EXTENSION	Read metadata for a specific AET extension
CRM_PS_DBA_GET_EXTENSION_LIST	Returns a list of AET extensions
CRM_PS_DBA_GET_MODEL	Read a specific DBA model
CRM_PS_DBA_GET_MODEL_LIST	Returns a list with all active DBA model headers

Data Protection

End of Purpose Check in SAP CRM

Social Services provides an end of purpose (EoP) check for business partner data when you execute the EoP check in SAP CRM. The EoP check in SAP CRM is organized centrally for all types of CRM business transactions (One Order Framework).

- The EoP check for Social Services is supported by the specific class CL_CRM_PS_4S_EOP_CHECK that is delivered with the handler class PSSC (*1Order -Social Services*) in the CRM Customizing settings under *CRM Cross-Application Components* > *Data Protection* > *Define Handler Class for Application Objects*.
- The Social Service business objects (BUS2000280, BUS2000281, BUS2000290, BUS2000292) are delivered as available application objects for the EoP check in the CRM Customizing settings under *CRM Cross-Application Components* > *Data Protection* > *Define Available Application Objects*.

For more information about the EoP check in SAP CRM, see the section Data Protection [page 35].

End of Purpose Check in SAP ERP

In SAP ERP Social Services provides the EoP check for business partner data, which is integrated using a RFC function module when you execute the EoP check in SAP CRM.

The data protection Customizing settings for business partners in SAP ERP are provided under *Cross-Application Components* > *Data Protection* > *Blocking and Unblocking of Data* > *Business Partner*

- The application entry PSSC (*Social Services*) is delivered for the EoP registration in the Customizing activity *Define and Store Application Names for EoP Check*.
- The entry PSSC is delivered covering the RFC function module PSSC_EOP_BUPA_CHECK for the EoP check in the Customizing activity *Define Application Function Modules Registered for Archiving Check*.
- In the Customizing activity *Define RFC Destinations of Systems Connected to Master System* you must configure a RFC destination to your SAP CRM system to support the EoP check triggered by the master system SAP CRM.

> **Note**
>
> Make sure that you also create a RFC destination from CRM to ERP in the respective Customizing settings for SAP CRM

For more information about data protection in SAP ERP, see SAP Library for SAP ERP Central Component on SAP Help Portal at help.sap.com/ecc <*Choose Release*> ▶ *Application Help* › *SAP ERP Cross-Application Functions* › *Cross-Application Components* › *Data Protection* › *Deletion of Business Partner Data* ◀.

9.4 Public Sector: Grantor

A grantor program is a group of related activities designed to achieve specific objectives. Programs have distinct sources of funding and commonly require separate reporting to external users. Programs are broken down by the grantor into hierarchy levels, for internal management purposes.

A grantor application is a submission by an applicant for funding a grantor from a grant program.

A grantor agreement outlines the conditions of the undertaking between a grantor and a prospective recipient of a grant, and describes the obligations of each. An agreement may take the form of a legal contract.

A grantor claim is a request from the grantee for payment based on accounting for incurred expenses or prepayment.

User Management and Authentication

The grantor application uses the user management and authentication mechanisms of SAP NetWeaver; in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 this application.

User Management

Table 414

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialog user	No	Mandatory user who can access service transactions. To be maintained by an SAP CRM system administrator.
SAP NetWeaver Business	Personal user	No	Dialog user	No	Mandatory user who can access SAP NetWeaver BW applications.

System	User	Delivered?	Type	Default Password	Description
Warehouse (SAP NetWeaver BW)					To be maintained by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user who can process background tasks. To be maintained by an SAP CRM system administrator.
SAP ERP	Personal or technical user	No	Dialog or system user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the remote function call (RFC) destination, the user can be an individual user or a system RFC user. To be maintained by an SAP ERP system administrator. Needed only if SAP ERP is used.

Authorization Objects

The following authorization objects exist, allowing for a specific authorization depending on the type of the grantor project involving the employee responsible as a central entity:

Table 415

Authorization Object	Description
CRM_GAP	Grantor Application
CRM_GMP	Grantor Program
CRM_GAG	Grantor Agreement
CRM_GCL	Grantor Claim

Other generic authorization objects may apply, such as CRM_ORD_OP (*CRM Order – Own Documents*) and UIU_COMP (*UIU – Component Access Authorization Check*).

If SAP ERP is used and an RFC user is created, this RFC user should be granted a profile that contains the following authorization objects and values:

For Funded Program:

Table 416

Authorization Object	Field 1	Value 1	Field 2	Value 2	Field 3	Value 3
S_RFC	RFC_TYPE	FUGR	RFC_NAME	CRM0	ACTVT	16
S_RFC	RFC_TYPE	FUGR	RFC_NAME	ERFC	ACTVT	16
S_RFC	RFC_TYPE	FUGR	RFC_NAME	ARFC	ACTVT	16

Authorization Object	Field 1	Value 1	Field 2	Value 2	Field 3	Value 3
F_FMMD_MES	FM_AUTHACT	01	FM_FIKRS	Customer-dependent	FM_AUTHGRM	Customer-dependent
F_FMMD_MES	FM_AUTHACT	02	FM_FIKRS	Customer-dependent	FM_AUTHGRM	Customer-dependent
F_FMMD_MES	FM_AUTHACT	03	FM_FIKRS	Customer-dependent	FM_AUTHGRM	Customer-dependent

For Earmarked Funds/Billing (AP/AR and PSCD Scenario):

Table 417

Authorization Object	Field 1	Value 1	Field 2	Value 2	Field 3	Value 3
S_RFC	RFC_TYPE	FUGR	RFC_NAME	ERFC	ACTVT	16
S_RFC	RFC_TYPE	FUGR	RFC_NAME	GTR_CRM_DOC_ERP_PROXY	ACTVT	16
S_RFC	RFC_TYPE	FUGR	RFC_NAME	ARFC	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL	Customer-dependent	Customer-dependent	Customer-dependent	Customer-dependent
F_FUNDSRES	BUKRS	Customer-dependent	FMRE_BLTYP	060	FMRE_BLART	Customer-dependent
F_FUNDSRES	BUKRS	Customer-dependent	FMRE_BLTYP	050	FMRE_BLART	Customer-dependent
F_FUNDSRES	BUKRS	Customer-dependent	FMRE_BLTYP	040	FMRE_BLART	Customer-dependent
F_FICB_FKR	FM_AUTHACT	10	FM_FIKRS	Customer-dependent	N/A	N/A
F_FMMD_MES	FM_AUTHACT	10	FM_FIKRS	Customer-dependent	FM_AUTHGRM	Customer-dependent
F_FMSPLITG	FMSP_ACTVT	7	FMSP_BEGRU	N/A	N/A	N/A

Network and Communication Security

The network topology for the grantor application is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in *SAP NetWeaver Application Server ABAP Security Guide* also apply to this application.

Communication Channel Security

The following communication channels are used:

- Remote function calls (RFCs)

- Business documents (BDocs)
- ABAP Structured Query Language (SQL) for the connection to the database

Communication Destinations

Table 418

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using SAP GUI for Microsoft Windows to CRM server	DIAG	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions.
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions.
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data
ERP server to CRM server	RFC	System ID, client, and host name, and all application data	System information and ERP data
CRM server to SAP NetWeaver BW server	RFC	System ID, client, and host name, and all application data	System information and CRM data
CRM Server to Internet Pricing and Configurator (IPC) (Necessary only if IPC runs on a separate installation. See SAP Note 855455.)	RFC	Pricing conditions	System information and CRM data

More Information

You can use Web requests to apply for grants over the Internet using an application form. For information on security-relevant settings, see section Web Requests [page 350].

9.5 Web Requests

You can use CRM web requests to generate XML-based request forms. Once you have filled out and submitted these forms, the system creates a SAP CRM business transaction, the form (as an XML file) and a link between both objects.

Currently, the web request is available for the following business transaction categories:

- Service Request (`BUS2000116`)
- Grantor Application (`BUS2000270`)
- Grantor Claim (`BUS2000272`)
- Social Application (`BUS2000280`)

For more information, see SAP Library on SAP Help Portal at help.sap.com/crm > *<Choose a release>* > *Application Help* > *Service* > *Web Requests* .

Online vs. Offline Scenario

Web request form data can be transferred to the SAP CRM System in an online or offline mode.

In the **online scenario**, the form is provided and displayed in a browser. You can choose between the two different layout categories Business Server Page (BSP) application (BSP) and Adobe Interactive Form (Web Dynpro with ADOBE Forms). You can access the form online using the Internet browser, fill it out and submit it. When you submit the form, this triggers creation of a SAP CRM business transaction. The form data is stored in XML format in the Knowledge Provider (KPro) and linked to the business transaction.

Recommendation

We recommend only using the online scenario in a secure network zone (such as a company's intranet). If you require input from the Internet to create a SAP CRM web request-based form, we recommend using the offline scenario as described above, for example in conjunction with a web server that stores the forms and converts them to XML content that is then used to create SAP CRM web requests).

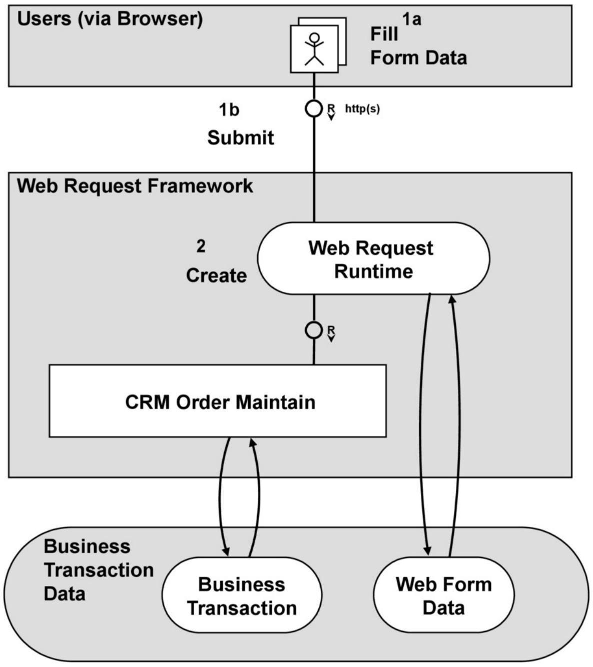


Figure 32: Fig.: Online Web Request Creation

In the **offline scenario**, completed forms are transferred as XML files to the SAP CRM System. The CRM process does not include creating the XML file. You can decide how you want to create XML files. The XML file (string) is transferred by calling the RFC function module `CRM_WEBREQ_EXTERN_CREATE`. When importing the XML file, the SAP CRM system creates a business transaction. The form data is stored in the Knowledge Provider (KPro) and connected to the business transaction.

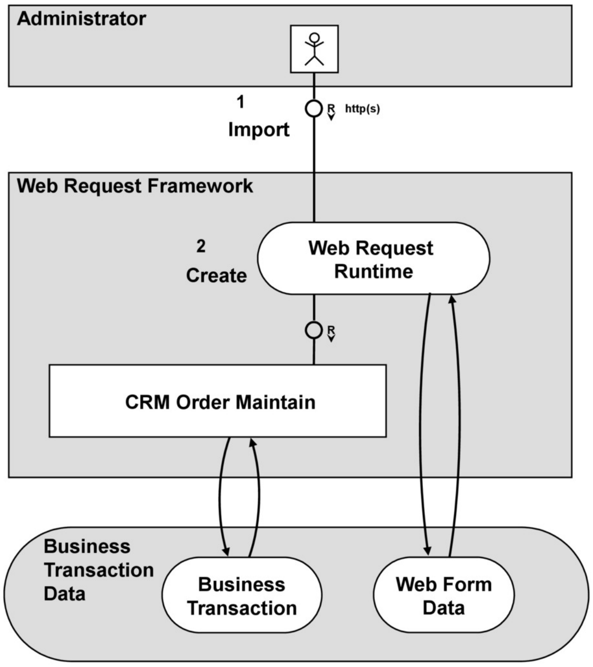


Figure 33: Fig.: Offline Web Request Creation

The figures above show that step 2 is identical in both scenarios. Security recommendations relating to this step are specified in section *Common Security Aspects*. Only step 1 is different in both scenarios. Recommendations for the online scenario are covered in section *Security Aspects in Online Scenarios* and for the offline scenario in section *Security Aspects in Offline Scenarios*. From a security perspective, the offline scenario has to be regarded as more secure because users do not have direct access to the SAP CRM System. For example, a possible denial-of-service attack to the form would have no negative impact on the SAP CRM System, if the form is provided on a dedicated web server and its data is imported to the SAP CRM System as an XML file at a subsequent stage.

When using the online scenario, you must adhere to common security recommendations for Internet scenarios. This security guide section only covers the special aspects for the SAP CRM web request.

Common Security Aspects

Authorizations

To create a business transaction, you must have the relevant authorizations. For more information, see SAP Library on SAP Help Portal at help.sap.com/crm › *<Choose a release>* › *Application Help* › *Basic Functions* › *Business Transaction* › *Authorization Check in Business Transactions*.

In addition, the CRM Web Request uses other authority objects during creation/change/display. The respective sections of this document describe how to define the authorizations for the online and the offline scenario.

Activation of CRM Web Request Categories

You can activate or deactivate your CRM Web request categories. If your category is activated, it can be executed (by authorized users). If your category is deactivated, the behavior depends on the environment and the client role (see table).

You can use the activation/deactivation flag to deactivate certain web request categories. These categories cannot be executed in productive systems. This also requires the web request categories that are delivered by SAP as examples to be deactivated as a default (however, you can easily activate these as required).

Table 419

Request Category	Environment	Activity	Client Role	Result
Activated	<all>	<all>	<all>	possible
Deactivated	WebClient UI	Create	<all>	Not possible (deactivated request categories are not shown)
		Search		Not possible (deactivated request categories are not available as search values)
		Change / Display	T (Test) C (Customizing) D (Demo) E (Training / Education) S (SAP Reference)	Possible, but warning is displayed in form
			P (Productive)	Not possible
	URL (Internet Access) (& Test View in Customizing)	Create	T (Test) C (Customizing) D (Demo) E (Training / Education) S (SAP Reference)	Possible, but warning is displayed in form
			P (Productive)	Not possible

Important SAP Note

Table 420

Title	SAP Note	Comment
CRM Web Request: Not Possible to Select Sample Request	1513117	Sample web request categories for Social Services and e-government are set to non-active in the standard system shipped.

Security Aspects in Online Scenarios

Authorizations

The CRM web request has a separate authority object CRM_VIEW. Users creating a web request require authorization for this object. The authorizations differ slightly between the online and offline scenario. In the online scenario, you use this authorization object to process web requests in SAP CRM. This involves form-supported entry and processing of requests on the Internet. An authorization check is performed to see whether the user can access certain request category views to change, display or create them. This check takes place when you access a form on the Internet.

Table 421

Authorization Object	Field	Value	Description
CRM_VIEW	ACTVT	01 (Create) 02 (Change) 03 (Display)	Activity Request
	WEBRQ_TYPE	<CRM Web Request Category>	Request Category
	WEBRQ_BGR	<Authorization group>	Authorization Group (Instead of Assigning Each Web Request Category Separately)
	WEBRQ_USE	View Usage of Your SAP CRM Web Request Category (see Check Table CRMC_RQV_USAGE)	Usage of Request Category View

User Management

To create a web request using the Internet, you require a user (user type: dialog) in the SAP CRM System. This SAP user must have the necessary authorizations to create a web request and the corresponding business transaction (see section *Authorizations*).

The identification can either be performed with the user name or with an alias (= Internet user). You can define which of these two options is admissible in the Internet Communication Framework (ICF) settings of the service for a web request.

ICF Configuration

When generating the layout of a SAP CRM web request category view of layout category BSP a BSP application is generated that is also entered as a service in the Internet Communication Framework (transaction SICF). From a security perspective, the following aspects should be taken into consideration:

- Make sure that you restrict the access of an ICF service for a CRM web request only to the permitted group of users!
- Make sure that you deactivate the ICF services for your CRM web requests that you no longer want to use.

For more information see SAP Library for SAP NetWeaver on SAP Help Portal at *Internet Communication Framework* [external document] and the *Security Guide of ICF* [external document].

BSP Only

We recommend two settings for the **BSP settings**:

- Usage of the HyperText Transfer Protocol by SSL HTTPS (and not HTTP) to transmit encrypted data to and from the user’s browser.
- Set the BSP application to *stateless* (not *stateful*) that no session is kept after the data has been sent to the user’s browser (see *Stateless BSP Applications* [external document]).

For more information see SAP Library for SAP Web Application Server on SAP Help Portal at *Business Server Pages* [external document] and at *Security Aspects for BSP* [external document].

The web request framework offers an integrated **input validation** of the field contents in the request forms. To use this feature, you have to ensure that all of your fields in the request data structure are associated with DDIC objects. The system only performs the input validation if you use DDIC objects when defining the fields.

All field content that a user enters in a web request form is automatically encoded (using html encoding). This **input encoding** is done to prevent persistent/stored cross-site scripting (XSS).

Adobe Only

When using the layout category `Web Dynpro with ADOBE Forms` you can always use the same **Web Dynpro application** `CRM_WEBREQ_IAF` that is delivered by SAP. You only need to create a separate application if the functionality of this Web Dynpro application is not sufficient.

For more information about the security settings, see the SAP NetWeaver Security Guide at *Web Dynpro ABAP Security Guide* [external document].

Security Aspects in Offline Scenarios

Authorizations

As of CRM 7.0 EhP1, a different authority object is checked in the offline scenario. If the switch `CRM_WR_1` is active and used in your business function(s), the system checks the new authority object. If the switch is not active, the old object is used.

If the **switch CRM_WR_1 is active,** the CRM web request has a separate authority object `CRM_VIEW`. If you want to execute the external interface (RFC function module) , you must have authorizations for this object. The authorizations differ slightly between the online and offline scenario. In the offline scenario, the system checks whether a user is allowed to create a web request of a certain web request category based on the imported form as an XML file.

Table 422

Authorization Object	Field	Value	Description
`CRM_VIEW`	`ACTVT`	`01 (Create)`	Activity
	`WEBRQ_TYPE`	`<CRM Web Request Category>`	Request Category
	`WEBRQ_BGR`	`<Not Checked>`	Not Relevant in Offline Scenario
	`WEBRQ_USE`	`<Not Checked>`	Not Relevant in Offline Scenario

If the **switch CRM_WR_1 is not active** the system uses the authority object `CRM_SEO` for CRM web requests. It checks if a user executing the external interface (RFC function module) has the necessary authorizations.

Table 423

Authorization Object	Field	Value	Description
`CRM_SEO`	`ACTVT`	`45 (Allow)`	Activity

External Interface (RFC Call)

The function module `CRM_WEBREQ_EXTERN_CREATE` imports web request form data from an external system to the SAP CRM System.

When using the external interface (= RFC function module `CRM_WEBREQ_EXTERN_CREATE`) to import XML files to the SAP CRM System, make sure that you grant the users the following authorizations:

Table 424

System Environment	Authorization Object	Use
RFC Client System (if it is a SAP system)	`S_ICF`	This authorization object controls which RFC destinations a user is allowed to use.
RFC Server System(the called system is the SAP CRM System)	`S_RFC`	Maintain the function group that contains the RFC function modules you want to allow a user to call.If the RFC function module `CRM_WEBREQ_EXTERN_CREATE` is used, the default function group is `CRM_WEBREQ_EXTERN`.

9.6 Investigative Case Management

The technical system landscape of the Investigative Case Management application is based on the technical system landscape of SAP Customer Relationship Management (SAP CRM).

Depending on the business process used, the technical system landscape can contain additional applications and systems. For example, business process *Managing Major Crimes* involves the following additional applications:

- Collaboration Projects (cProjects)

  cProjects can be installed as an ABAP add-on.
- Defense Forces & Public Security (DFPS)

  DFPS is running on SAP ERP.

Note that cProjects and DFPS are technically independent of each other.

Moreoever, you can search for predefined Investigative Case Management objects using SAP NetWeaver Enterprise Search.

For more information about the technical system landscape of each component, see the following guides:

Table 425

Technical System Landscape	Guide	Guide Location
Investigative Case Management application and the underlying components, such as SAP CRM and SAP NetWeaver	*Security Guide for SAP Customer Relationship Management*	Not applicable
System landscape with SAP NetWeaver Enterprise Search	*SAP NetWeaver Enterprise Search Security Guide*	help.sap.com/nwes
Integration with SAP NetWeaver Enterprise Search	*Security Guide for SAP Customer Relationship Management*	Not applicable
Technical system landscape of DFPS	*SAP ERP Central Component Security Guide*	service.sap.com/securityguide

Technical System Landscape	Guide	Guide Location
Technical system landscape of cProjects	*SAP Portfolio and Project Management Security Guide*	service.sap.com/securityguide

Security Aspects of Data, Data Flow and Processes

The figures below shows an overview of the data flow in the business process, *Managing Major Crimes*:

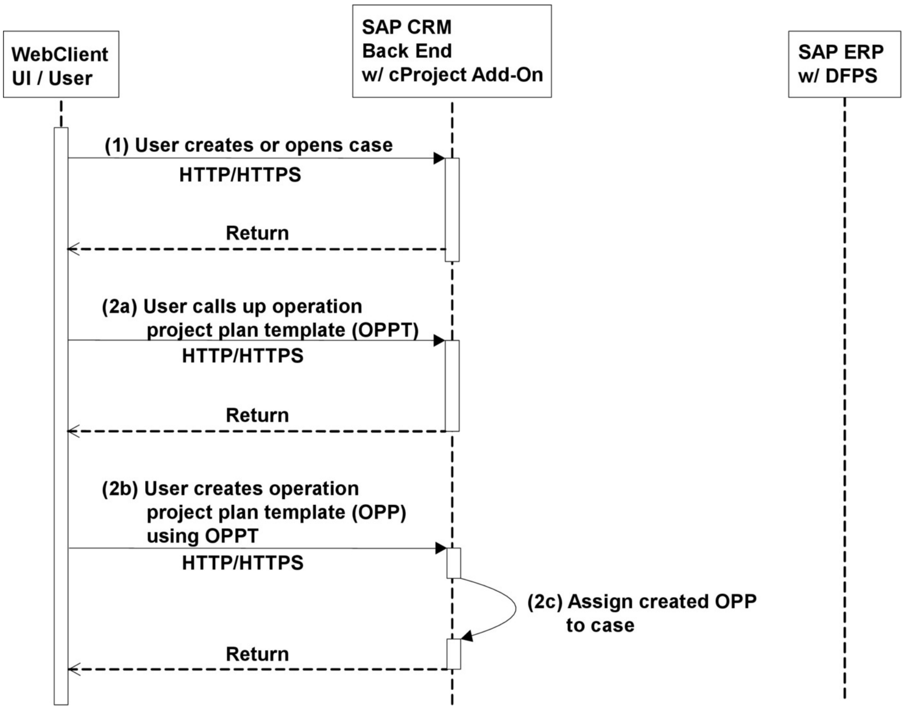

WebClient UI / User
SAP CRM Back End w/ cProject Add-On
SAP ERP w/ DFPS
(1) User creates or opens case
HTTP/HTTPS
Return
(2a) User calls up operation project plan template (OPPT)
HTTP/HTTPS
Return
(2b) User creates operation project plan template (OPP) using OPPT
HTTP/HTTPS
(2c) Assign created OPP to case
Return

Figure 34: Overview of Process Steps for Investigative Case Management: Part 1

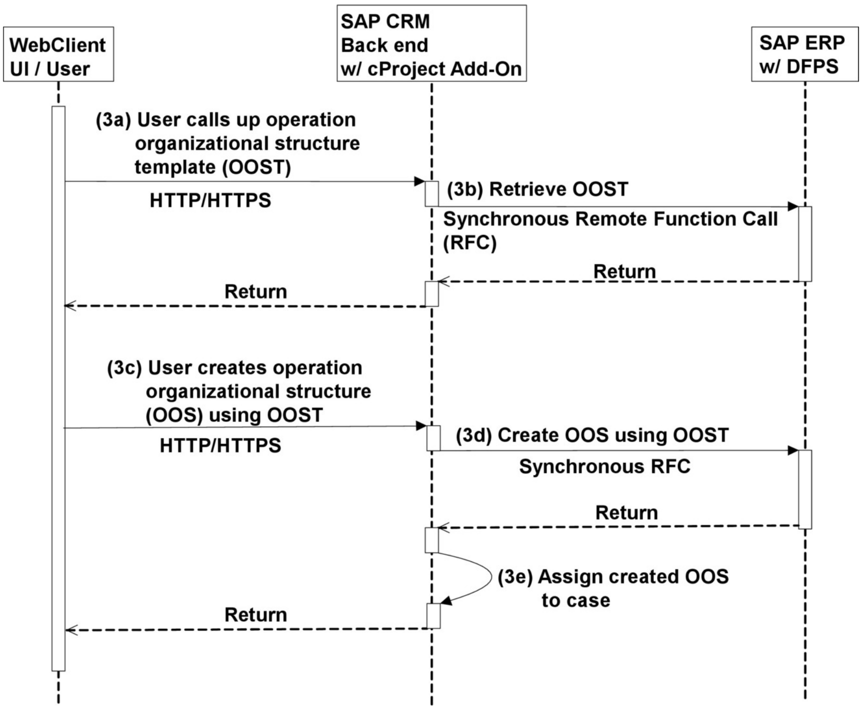

WebClient UI / User
SAP CRM Back end w/ cProject Add-On
SAP ERP w/ DFPS
(3a) User calls up operation organizational structure template (OOST)
HTTP/HTTPS
(3b) Retrieve OOST
Synchronous Remote Function Call (RFC)
Return
Return
(3c) User creates operation organizational structure (OOS) using OOST
HTTP/HTTPS
(3d) Create OOS using OOST
Synchronous RFC
Return
(3e) Assign created OOS to case
Return

Figure 35: Overview of Process Steps for Investigative Case Management: Part 2

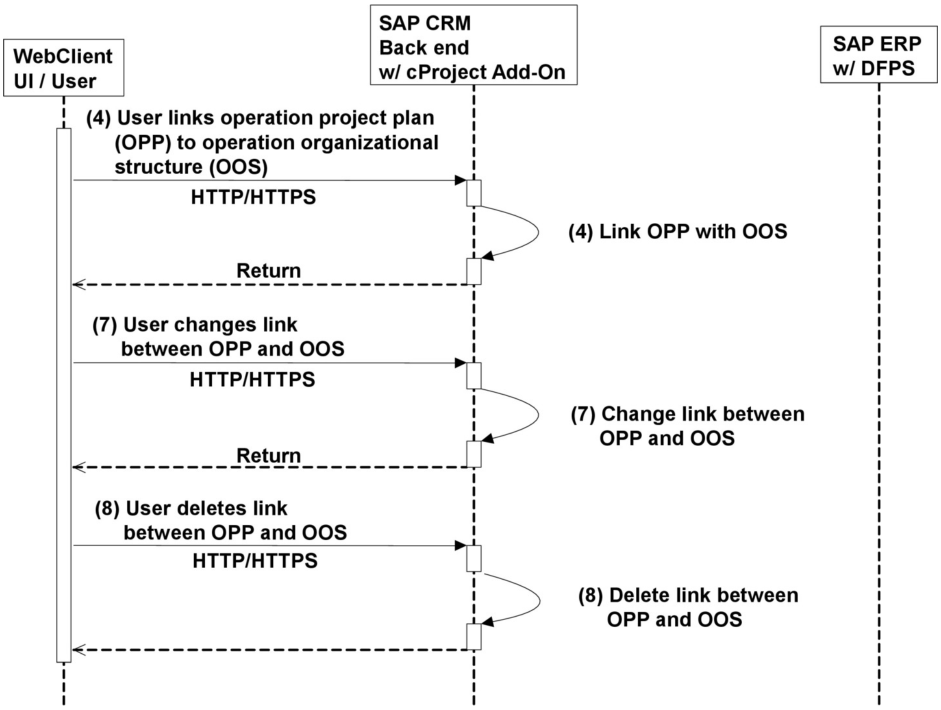

WebClient UI / User
SAP CRM Back end w/ cProject Add-On
SAP ERP w/ DFPS
(4) User links operation project plan (OPP) to operation organizational structure (OOS)
HTTP/HTTPS
(4) Link OPP with OOS
Return
(7) User changes link between OPP and OOS
HTTP/HTTPS
(7) Change link between OPP and OOS
Return
(8) User deletes link between OPP and OOS
HTTP/HTTPS
(8) Delete link between OPP and OOS

Figure 36: Overview of Process Steps for Investigative Case Management: Part 3

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

Table 426

Step	Description	Security Measure
1	User creates or opens case	Follow the guidelines for ensuring transport layer security of Internet protocols. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform > *<Choose relevant release>* > *Security Information* > *Security Guide* > *Network and Communication Security* > *Transport Layer Security* .
2a	User calls up operation project plan template	See security measure for step 1
2b	User creates operation project plan using operation project plan template	See security measure for step 1
2c	Assign created operation project plan to case	Not applicable
3a	User calls up operation organizational structure template	See security measure for step 1
3b	Get operation organizational structure template	See subsection *Communication Channel Security* below.
3c	User creates operation organizational structure using operation organizational structure template	See security measure for step 1
3d	Create operation organizational structure using operation organizational structure template	See security measure for step 1
3e	Assign created operation organizational structure to case	Not applicable
4	User links operation project plan to operation organizational structure	See security measure for step 1
5	Add further operation project plans (steps 2a – 2c)	Not applicable
6	Add further operation organizational structures (steps 3a – 3e)	Not applicable
7	User changes links between operation project plans and operation organizational structures	See security measure for step 1
8	User deletes links between operation project plans and operation organizational structures	See security measure for step 1

User Administration and Authentication

Investigative Case Management uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver 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 the Investigative Case Management application.

User Management Tools

The following table shows the tools to use for user management and user administration in Investigative Case Management:

Table 427

Tool	Description	Prerequisites
User and role administration with SAP NetWeaver AS ABAP: *User Maintenance* (`SU01`) transaction and the profile generator (`PFCG`) transaction	User accounts in Investigative Case Management must be directly associated with the *Detective* PFCG role. This association binds the user to the dynamic authorization subsystem of Investigative Case Management. For more information, see SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* › *Security* › *Identity Management* › *User and Role Administration of Application Server ABAP* › *Administration of Users and Roles* ◀.	You have assigned all Investigative Case Management users to the *Detective* PFCG role.

User Types

For Investigative Case Management, it is necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively change their passwords on a regular basis, but users who process background jobs do not.

For Investigative Case Management, there are the following types of users:

- Users with the standard detective role

  These users are subject to the dynamic authorization rules and rights outlined in the *Authorizations* section below. The authorization model requires that these users be directly associated with the *Detective* PFCG role (using the `SU01` or `PFCG` transactions).

- Users with an administrative role

  These users are granted universal rights over objects governed by the dynamic rules and rights outlined in the *Authorizations* section below.

For more information about these user types, see *User Types* section in the *SAP NetWeaver AS ABAP Security Guide*.

Authorizations

Investigative Case Management uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver AS Security Guide ABAP* also apply to Investigative Case Management. For more information, see the Authorizations [page 25] section.

If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). For more information, see the Access Control Engine [page 324] section.

Standard Roles

The following table shows the standard roles that are used and delivered in Investigative Case Management:

Table 428

Role	Description
SAP_CRM_ICM_PROFESSIONAL	This is the Investigative Case Management composite PFCG role, which contains the individual PFCG roles below.
SAP_CRM_UIU_ICM_PROFESSIONAL	This PFCG role contains authorizations for a professional user working with the Investigative Case Management application in the WebClient UI. It contains the Investigative Case Management-specific authorization objects for the *Security Level* and *Hide* functions. This role can be used to derive the PFCG roles a customer needs.
SAP_CRM_ICM_OOS_EXTERN	This PFCG role contains authorizations for requesting operation organizational structure (OOS) information from an external ERP system.

Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by Investigative Case Management::

Table 429

Authorization	Field	Value	Description
CRM_ICMADM	ACTVT	W1 W2 W3	Each value specifies a particular authorization for an activity. W1 grants the authorization to add and remove partners from the *Staff & Units* assignment block of the Investigative Case Management case entity. W2 grants the right to toggle the hidden flag for the Investigative Case Management case entity. W3 grants the right to toggle the relationship expunge date for the Investigative Case Management application.
CRM_ICMCAS	ICM_SECLVL	Allowed customized security levels for ICM	An instance of this object defines the security level for a case type. For example, the combination **ICM_SECLVL = 50** and **ICM_CASTYP = ICMC** grants the user or owner of the static authorization object instance
	ICM_CASTYP	Available case type for Investigative Case Management	

Authorization	Field	Value	Description
			a security level of 50 for cases of type ICMC.
CRM_ICMLEA	ICM_SECLVL	Allowed customized security levels for Investigative Case Management	An instance of this object defines the security level for a lead type. For example, the combination **ICM_SECLVL = 50** and **ICM_LEATYP = ICML** grants the user or owner of the static authorization object instance a security level of 50 for cases of type ICML.
	ICM_LEATYP	Available lead type for Investigative Case Management	
CRM_ICMOPE	ICM_SECLVL	Allowed customized security levels for Investigative Case Management	An instance of this object defines the security level for an operation type. For example, the combination **ICM_SECLVL = 50** and **ICM_OPETYP = OPR** grants the user or owner of the static authorization object instance a security level of 50 for operations of type OPR.
	ICM_OPETYP	Available operation type for Investigative Case Management	
CRM_ICMINC	ICM_SECLVL	Allowed customized security levels for Investigative Case Management	An instance of this object defines the security level for an incident type. For example, the combination **ICM_SECLVL = 50** and **ICM_INCTYP = ICNC** grants the user or owner of the static authorization object instance a security level of 50 for incidents of type ICNC.
	ICM_INCTYP	Available incident type for Investigative Case Management	
CRM_ICMREL	ICM_SECLVL	Allowed customized security levels for Investigative Case Management	An instance of this object defines the security level for a relationship type. For example, the combination **ICM_SECLVL = 50** and **ICM_RELTYP = Z001** grants the user or owner of the static authorization object instance a security level of 50 for relationships of type Z001.
	ICM_RELTYP	Available relationship type for Investigative Case Management	

Authorization	Field	Value	Description
CRM_ICMBP	ICM_SECLVL	Allowed customized security levels for Investigative Case Management	An instance of this object defines the security level for business partners. For example, the setting **ICM_SECLVL = 50** grants a security level of 50 for business partners.
CRM_ICMBPP	ICM_SECLVL	Allowed customized security levels for Investigative Case Management	An instance of this object defines the security level for business partners. For example, the setting **ICM_SECLVL = 50** grants a security level of 50 for business partner profiles.
CRM_ICMRLA	ACTVT	Allowed customized ACTVT entries: 1 Create 2 Change 3 Display W3 Toggle Expunge Data	This object is used to determine what activities can be performed on a relationship.

Standard Static Authorization

The role of standard static authorizations in Investigative Case Management is to grant specific rights to the user or owner of the static authority object.

The table of static objects defines the unique static authorization object used in Investigative Case Management for this purpose: CRM_ICMADM.

The values of the CRM_ICMADM field are described in the static authorization object table.

Other static authorization objects are used with dynamic authorization. For more information, see the *Dynamic Authorization* section below.

Dynamic Authorization

Dynamic authorization is used in Investigative Case Management to define access rights for users to given Investigative Case Management application objects. Each right is defined as the association of an object type, a rule, a user group, and action group. The main part of a right is the rule, which defines the authorization relationship between an object type and a user. The association of an action group allows you to define similar rights, which grant different access types. For example, a right may allow for read-only access to an object, while an identical definition, with the exception of the action group, may allow for write access to the object.

The Customizing and implementations of Investigative Case Management authorization rules for the detective role are delivered with the Investigative Case Management application.

Investigative Case Management includes the following authorization business rules:

- Security level rule

  The security level rule is used to provide a broad level of authorization. The rule grants access rights to users who have a security level for a given Investigative Case Management application entity type that is higher than or equal to the security level of a given instance of the entity type. The security level assignment is done using the security level static authorization objects discussed in the *Standard Static Authorization* section above.

- Staff and units rule

  The staff and units rule is used to provide a more granular level of authorization. The rule grants access rights to users who belong to entity instance *Staff & Units* in the Investigative Case Management application.
- Hidden rule

  The hidden rule is a composite rule. This rule revokes access rights from users who typically have access using the security level rule unless they also belong to the staff and units rule.

To comply with security requirements and standards, the *Detective* business role is associated to a technical profile that checks whether the ACE restrictive mode is enabled. If the ACE restrictive mode is not enabled in the target system, the user attempting to log on with the standard *Detective* role is redirected to an error page. This indicates that ACE was not properly configured for Investigative Case Management.

Dynamic Authorization Tools

The following tools and Customizing activities are used to configure the dynamic authorization subsystem:

Table 430

Tool	Detailed Description	Prerequisites
Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Maintain General Parameters*	General Maintenance tool. This tool is used to set ACE parameters such as ACE restrictive mode.	You have read the prerequisites activity and are aware of the required parameters for Investigative Case Management.
Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Rules* > *Create Rules*	Rule definition tool. This tool is used to edit the cross-client tables that are used to define the ACE rules, ACE actions, ACE object-types, and rule implementation classes.	N/A
Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Create Rights*	Right definition tool. This tool is used to define the ACE work package, ACE object assignment, ACE user group assignment, and definitions of rights.	You have performed rule customization.
Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Activate/Deactivate Work Packages and Rights*	This tool is used to activate and deactivate the ACE work package and rights.	You have defined the ACE work package and rights.
Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Analyze Runtime Data*	This tool is used to analyze ACE runtime data.	You have activated a work package and its associated rights.
Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Update User- and Object Context*	This tool is used to update ACE user and object contexts. Although the ACE dispatcher runs at object change and user logon, it may	A work package and its associated rights must be active.

Tool	Detailed Description	Prerequisites
	become necessary to update the rights for a user or object. This tool may be used to perform this task.	

Business Role

All Investigative Case Management application users should be assigned to a business role that is derived from the standard *Detective* business role.

The standard *Detective* business role is associated with the technical profile `DEFAULT_ICM`, which is used to determine if the ACE restrictive mode is enabled. If a user tries to log on using the *Detective* business role, this check ensures that ACE restrictive mode is enabled. If the restrictive mode is disabled, the application redirects users to an error page containing a message, which prompts them to configure ACE according to the Investigative Case Management security standards.

The *Detective* business role provides the necessary UI configuration that the Investigative Case Management user needs to navigate within the Investigative Case Management application.

The *Detective* business role can be assigned to a user in the following ways:

- Using the user's business partner and the organizational maintenance transaction `PPOMA_CRM`. The business role can be assigned to an organization position with the *Enhanced Object Description* interface. This is the recommended approach.
- Using the user management transaction `SU01` and the user parameter tab of the tool. The user parameter `CRM_UI_PROFILE` is used to assign the business role.
- Using the user management transaction `SU01` and the assignment of a PFCG role to a *Detective* business role.

PFCG Roles

A standard PFCG composite role has been created that should be used to assign users to the ACE work package `SAP_CRM_ICM_PROFESSIONAL`.

For users to be recognized as being assigned to the PFCG role with respect to the ACE, users must be assigned to the PFCG role directly. This can be done in the following ways:

- Add the user to the user maintenance tab in the `PFCG` transaction. This is the recommended approach.
- Add the PFCG role to the user role tab in the `SU01` transaction
- Assign the user within the organizational model to a position that has an appropriate business role assigned.

Once the user is added to the PFCG role, the ACE context needs to be refreshed. For more information, see the *User and Object Context Update* section.

The PFCG role is assigned to the ACE user group `SAP_ICM_PROFESSIONAL`.

ACE Configuration and Customizing

The dynamic authorization model relies on standard Customizing to provide the default dynamic authorization rights. This Customizing can be enhanced by the customer to define and implement new rules and rights.

The ACE rules are built using implementation classes (implemented in ABAP) and a number of Customizing definitions. These rules are defined for a specific set of business objects, which are then assigned to the rules.

In Investigative Case Management, the ACE rules apply to the following business objects:

- ICMCASE
- ICMLEAD

- ICMOPERATION
- ICMINCIDENT
- ICMRELATIONSHIP
- ICMBUSINESSPARTNER
- ICMBUSINESSPARTNERPROFILE
- VEHICLECRM

These objects are specifically assigned to the customized work package SAP_CRM_ICM.

The following sections describe each of the customized components of the ACE configuration.

The ACE Group

A customized ACE user group, SAP_ICM_PROFESSIONAL, has been created to assign the SAP_CRM_UIU_ICM_PROFESSIONAL PFCG role to the customized rights for the ACE work package SAP_CRM_ICM.

To assign users to the ACE group, the administrator must assign users to the PFCG role directly.

The ACE Actions and Action Group

The actions define the type of action assigned to the right. For example, an action could be read, write, or delete (standard actions).

The action group assigns actions under one grouping, which is used in the ACE right definition.

The ACE Work Package

A customized work package, SAP_CRM_ICM, has been created to assign the ACE user group SAP_ICM_PROFESSIONAL to Investigative Case Management rights. This group specifies which rights apply to the following ACE objects:

Table 431

Object	Description
ACCOUTCRM	ICM Business Partner
CASEMANAGEMENT	ICM Case and Lead
ICMBPPPROFILE	ICM Business Partner Profile
VEHICLECRM	ICM Location and Objects
ICMRELATIONSHIP	ICM Relationships
ONEORDER	ICM Operations and Incidents

The ACE work package is also assigned to the following rights, which are used to determine the authorization relationship between users and object instances:

Table 432

Right	Description
ICM_PRO_ACT_SECLVL	Operation and Incident Security Level Right
ICM_PRO_BPP_SECLVL	Business Partner Profile Security Level Right
ICM_PRO_BP_SECLVL	Business Partner Security Level Right

Right	Description
ICM_PRO_BP_STAFFU	Business Partner Staff & Units Right
ICM_PRO_CMG_SECLVL	Case & Lead Security Level
ICM_PRO_CMG_STAFFU	Case & Lead Staff & Units Right
ICM_PRO_LOC_BASE	Location Base Right
ICM_PRO_LOC_STAFFU	Location Staff & Units Right
ICM_PRO_REL_SECLVL	Relationship Security Level Right

The ACE Rules

The ACE rules are the building blocks of the ACE rights. They serve as a link between the technical implementation of the rules and the definitions of the ACE rights.

The following is a list of the ICM-specific rules:

Table 433

Rule	Description
ICM_CMG_SEC_LVL	Case & Lead Security Level and Hidden Rules
ICM_CMG_STAFFU	Case & Lead Staff & Units Rule
ICM_ACT_SEC_LVL	Operation & Incident Security Level and Hidden Rules
ICM_BP_SECLVL	Business Partner Security Level and Hidden Rules
ICM_BP_STAFFU	Business Partner Staff & Units Rule
ICM_BPP_SEC_LVL	Business Partner Profile Security Level and Hidden Rules
ICM_LOC_BASE	Location Base Rule
ICM_LOC_STAFFU	Location Staff & Units Rule
ICM_REL_SEC_LVL	Relationship Security Level Rule

The ACE Rights

The ACE rights define a relationship between an authorizable object, an ACE group, and a defined ACE rule. This relationship is then used when the ACE authorization subsystem checks object instances for authorization.

The rights created for Investigative Case Management are listed in the *ACE Work Package* section above.

Custom Rules and Rights

One of the main advantages of the ACE framework is that you can define the new customer rules and rights independent of existing ACE Customizing. You can also define rules and rights to replace existing ones.

The following sections describe the steps for defining and implementing customer-specific ACE rules and rights.

Rule Implementations

The ACE rules are implemented in ABAP using the following provided interfaces:

- `IF_CRM_ACE_ACTORS_FROM_OBJECT`

Starting with an object, this interface determines all actors related to this object.

- `IF_CRM_ACE_ACTORS_FROM_USER`

  Starting with a user, this interface determines all actors related to this user.
- `IF_CRM_ACE_OBJECTS_BY_FILTER`

  Finds all objects defined by a specific filter.

Once you have implemented these rules, you must register them in the ACE Customizing for them to be used as rules.

Custom ACE Rule Definitions

You must define the ACE rules in Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Rules* > *Create Rules*.

An ACE rule is the association of an object type, rule ID, rule description, actor type, actors for user rule implementation, actors for objects implementation, and an object by filter implementation.

Although it is possible to create new rules, the following generic rules exist to allow for simplified customization of rights:

Table 434

Rule	Description
`ICM_CMG_ADMIN`	Case & Lead Administrative Rule
`ICM_ONEORDER_ADMIN`	Operation & Incident Administrative Rule
`ICM_ACCOUNT_ADMIN`	Business Partner Administrative Rule
`ICM_BPP_ADMIN`	Business Partner Profile Administrative Rule
`ICM_LOCATION_ADMIN`	Location Administrative Rule
`ICM_REL_ADMIN`	Relationship Administrative Rule

➡ Recommendation

You can create custom rules, but this process can be time-consuming. Before you begin creating rules, we recommend running an in-depth analysis of existing rules to identify any rules that match the custom requirements.

Custom ACE Work Package

To assign custom ACE user groups to custom ACE rights, you must create a customer namespace work package. As is the case with standard Customizing, this work package must specify which rights apply to the ACE objects.

You can define a work package in Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Create Rights*.

Custom ACE User Group

To assign the users to the ACE rights, you must create a customer namespace ACE user group to associate the users to the ACE Rights in Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Create Rights*.

You can assign users to the ACE user group in the following ways:

- Direct user assignment
- Assignment using groups

- Assignment using PFCG role

Recommendation

Assign users using groups or PFCG roles. This type of user assignment allows changes to be made without the need to deactivate and reactivate the associated work package and rights. You can use a context update to ensure that the rights for the user have been updated.

Custom ACE Rights

You must create customer namespace rights to activate custom rules. You can also create custom rights using existing rule definitions and implementations.

To create rights, go to Customizing for *Customer Relationship Management* under *Basic Functions* > *Access Control Engine* > *Create Rights*.

The definition of a right is a combination of right ID, right description, object type, rule ID, user group ID, action group ID, and a validity period.

Network and Communication Security

The network topology for Investigative Case Management is based on the topology used by the SAP NetWeaver platform. For more information, see the Network and Communication Security [page 29] section.

Communication Channel Security

For the bidirectional communication between the Investigative Case Management in SAP CRM andDefense Forces & Public Security (DFPS) in SAP ERP, synchronous Remote Function Calls (RFCs) are used. Therefore, the general communication path between the CRM server and the ERP server mentioned in the UI Framework [page 310] section applies to application data specific to Investigative Case Management and to DFPS.

DFPS is called using remote function call (RFC). The communication between the Investigative Case Management application in SAP CRM and Defense Forces & Public Security (DFPS) is not based on the middleware between SAP CRM and SAP ERP. Therefore no system-based synchronization takes place.

Users can navigate from the Investigative Case Management application in the CRM system (WebClient UI) to the DFPS system (SAP GUI for HTML). The DFPS UI is called using SAP Internet Transaction Server (ITS); it is not displayed in-place.

Note

For the RFC communication, users require a corresponding user with the identical user name in the calling system. This applies to the SAP CRM system and the SAP ERP system.

In case of an integration with cProjects, no RFC is used because cProjects is run as an additional software component on the SAP CRM system and all calls to cProjects are done locally.

User can navigate from the Investigative Case Management application (WebClientUI) to cProjects (Web Dynpro for ABAP).

For communication between SAP CRM and SAP NetWeaver Enterprise Search, the general communication path mentioned in the UI Framework [page 310] section applies to models, templates, and search data specific to Investigative Case Management.

Communication Destinations

SAP does not deliver any RFC destinations for Investigative Case Management.

For all RFC calls mentioned below, we recommend using trusted RFCs with the same user in both systems. Be sure to grant the users the following authorizations:

- In the RFC client system (the calling system):
  - `S_ICF`: With this authorization object, you can decide which RFC destinations a user may use.
- In the RFC server system (the called system):
  - `S_RFC`: Maintain the function groups that contain the RFC function modules you want to allow a user to call.
  - `S_RFCACL`: Checked when trusted RFC is used. We recommend that you use the same user in both the calling and the called system. If you follow this recommendation set the field `RFC_EQUSER` to **Y**.

RFC calls from Investigative Case Management (CRM) to DFPS (ERP)

All RFC function modules in the DFPS system that are called have the namespace `/ISDFPS/` and start with `ICMOF_`. They are all contained in the function group `/ISDFPS/ICM_OF`. You have to enter this function group in the respective field of authorization for `S_RFC`.

These calls are used to create operation organizational structures (OOS), search for them, and retrieve their data.

Since no RFC destinations are delivered in the standard system, you have to create your own destination to DFPS in the investigative case management system. You then have to maintain this destination in Customizing.

> Note
>
> For more information about maintaining the destination, see Customizing for *Customer Relationship Management* under ▶ *Industry-Specific Solutions* › *Public Sector* › *Investigative Case Management* › *Cases and Leads* › *Setting Up DFPS Integration* ◀.

RFC calls from DFPS (ERP) to Investigative Case Management (CRM)

In the DFPS UI, the case ID to which an OOS is linked is shown. To obtain this ID, the RFC function module `CRM_ICM_CASE_AND_OPP_GET` is called. The same function module also has to be called in the case of archiving DFPS data.

The respective settings for the authorization object `S_RFC` in investigative case management are already maintained in the standard PFCG role (see above).

Other Security-Relevant Information

The standard settings in SAP CRM allow users to search for all business partners. To limit your searches to persons and organizations in investigative case management from the standard objects, see Customizing for *Customer Relationship Management* under ▶ *Industry-Specific Solutions* › *Public Sector* › *Investigative Case Management* › *Persons and Organizations* › *Exclude ICM Persons and Organizations from Account and Contact Search* ◀.

9.7 Telco Dealer Application

The telco dealer application is only designed to be used in a company intranet environment for company-owned dealers that work on the same system. The telco dealer application does not require explicit activation of the ICF services.

Since the application uses the Interaction Center (IC) WebClient, the component-specific guidelines for the IC WebClient in this guide apply. For more information, see Component-Specific Guidelines: Interaction Center [page 202].

Technical System Landscape

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

Table 435

Topic	Guide/Tool	Quick Link SAP Service Marketplace or SDN
Technical description for *Sales and Order Management in Dealer Channel* and the underlying technological components such as SAP NetWeaver	SAP for Telecommunications 2010 - Master Guide	service.sap.com/instguides

Network and Communication Security

The network topology for the telco dealer application is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide and in the Component-Specific Guidelines: Interaction Center [page 202] section of this guide apply to this application. For more information, also see the main Network and Communication Security [page 29] section in this guide.

Communication Destinations

In addition to the general paths used by SAP CRM, the telco dealer application also uses the following communication path:

Table 436

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to ERP server	HTTPS	Application data (XML)	Personal data

9.8 Sales and Order Management

You can use the Sales and Order Management scenario to sell postpaid and prepaid services and the industry's usual product bundle of services and goods. By providing these processes within the call center and the back office, two different customer channels are supported. The business scenario is integrated with SAP ERP Invoicing and SAP Convergent Charging to provide an end-to-end Order to Cash scenario. In the integrated scenario, the different type of data is replicated and synchronized across systems. To control the integration and to keep the data consistent, you may need access to the applications that store this data to restrict access to persons who are authorized to view this information only.

Note

For the Sales and Order Management scenario, the same guidelines apply as for the Quotation and Order Management scenario. The scenario uses the CRM Interaction Center. Therefore, the component-specific guidelines for the Interaction Center in this guide apply in addition to the information and recommendations in this section. For more information, see Component-Specific Guidelines: Interaction Center [page 202].

Techical System Landscape

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

Table 437

Topic	Guide/Tool	Quick Link SAP Service Marketplace or SDN
Technical description for *Financial Customer Care and Dispute Management* and the underlying technological components such as SAP NetWeaver	SAP for Telecommunications 2012 - Master Guide	service.sap.com/instguides

Authorizations

Standard roles used by the Sales and Order Management scenario:

Table 438

Business Role	PFCG Role	Description
ETC_IC	SAP_CRM_UIU_ETC_IC_AGENT	*Toll Collection IC Agent*
PROVIDER_IC	SAP_CRM_UIU_PROVIDER_IC_AGENT	*Provider IC Agent*
TELCO_IC	SAP_CRM_UIU_TELCO_IC_AGENT	*Telco: IC Agent Master Role*
PROV_SALES	SAP_CRM_UIU_PROVIDER_SALES	*Provider Sales and Order Management*

Standard Authorization Objects

The following table lists the security-relevant authorization objects that are used in the Sales and Order Management scenario. For more information, see SAP Library on SAP Help Portal at *http://help.sap.com/crm<Choose a release>* › *Application Help* › *Basic Functions* › *Business Transaction* › *Authorization Check in Business Transactions*.

Table 439

Authorization Object	Description
CRM_BA_CLS	Business Agreement: Business Agreement
CRM_ORD_LP	Visibility in the organizational model
CRM_ORD_TE	Order-Visibility in Territory
CRM_ORD_PR	Business Transaction Type
CRM_ORD_OE	Allowed organizational units
COM_PRD	Product Master: General Authorization
COM_PRD_CT	Product Master: Authorization for Category
CRM_PRVMA	Provider Master Agreement

`CRM_ISX_AD`	Allowance Definition and Allowance Definition Group

In addition, you can implement the BAdI CRM_ORDER_AUTH_CHECK to create enhancements for the authorization check in the business transaction. If the standard authorization concept provided is not sufficient, you can also use the access control engine (ACE). For more information, see the Access Control Engine section.

A further way that you can control access to the application is by using the authorization object `UIU_COMP`. This object allows you to dynamically hide certain links in the navigation bar of the CRM Web UI based on the user's authorization profile.

Table 440

Authorization Object	Authorization Fields
`UIU_COMP` (UIU: Component Access Authorization Check)	`COMP_NAME` (Component Name) `COMP_WIN` (Component Window Name) `COMP_PLUG` (Inbound Plug)

Network and Communication Security

The network topology for the Sales and Order Management scenario is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to this scenario. For more information, see the main Network and Communication Security [page 29] section in this guide.

Communication Destinations

SAP CRM and other application components (such as SAP Convergent Charging or SAP ERP) communicate through RFC-TCP/IP communication destinations encrypted with the SAP Cryptographic Library.

Table 441

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to ERP server	RFC	System ID, client, host name, and all application data	System information and CRM data
CRM server to Convergent Charging server	SOAP over HTTP/HTTPS	Application data (XML)	Web service user: username/ password

For the communication by means of RFC with the ERP system, we recommend that you use named users, that means, Contract Accounts Receivable and Payable (FI-CA) and CRM use the same user names.

This technical web user must correspond to a SAP CC user granted with the adequate roles and associated to a given catalog. For more information, see the security Guide SAP Convergent Charging.

Data Storage Security

Using Logical Path and File Names to Protect Access to the File System

Sales and Order Management stores data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs.

The following logical file name has been created with the following path to enable the validation of the physical file name:

Table 442

Program	Logical File Name Used by the Program	Logical Path Name Used by the Program
`CRM_FICA_MIG_PROVIDER_CONTRACT`	`FI-CA-MIG_FILE`	`FI-CA-MIG_ROOT`

Activating the Validation of Logical Path and File Names

These logical paths and file names are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physcial path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log. For more information, see the following references:

- SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ◀: Search for *Logical File Names*
- SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for the Application Server* › *Security Guides for the AS ABAP* › *SAP NetWeaver Application Server ABAP Security Guide* › *Special Topics* › *Protecting Access to the File System Using Logical Path and File Names* ◀
- SAP Library for SAP NetWeaver on SAP Help Portal at ▶ help.sap.com/nw_platform › *<Choose relevant release>* › *Application Help* › *Function-Oriented View* ◀: Search for *Security Audit Log*

9.9 Media: SAP Intellectual Property Management

SAP Intellectual Property Management (IPM), a solution in SAP for Media, is a comprehensive solution that covers the entire value creation chain for intellectual property. This includes the acquisition and creation of intellectual property, development of new media products, sale of licenses and rights, through to management of license revenues and royalties. SAP IPM also contains functions for maintaining business relationships with rights owners, licensors and licensees, actors or authors of intellectual property.

Important SAP Notes

The most important SAP Notes that apply to the security of the SAP IPM component are shown in the table below:

Table 443

Title	SAP Note	Comment
Potential disclosure and modification of persisted data	1482449	A malicious user can exploit IPM Mass Change database batch data loading reports using specially crafted inputs to execute arbitrary database commands to retrieve, modify, or remove data persisted by the system.

		The problem is caused by an SQL injection vulnerability. The code composes an SQL statement including strings that can be altered by a malicious user. The manipulated SQL statement can then be used to retrieve additional information from the database or to potentially modify it. **Please implement the correction instructions attached to the note**.
Potential disclosure and modification of persisted data	1482450	A malicious user can exploit IPM Mass Change template UI using specially-crafted inputs to execute arbitrary database commands to retrieve, modify, or remove data persisted by the system. The problem is caused by an SQL injection vulnerability. The code composes an SQL statement including strings that can be altered by a malicious user. The manipulated SQL statement can then be used to retrieve additional information from the database or to potentially modify it. **Please implement the correction instructions attached to the note.**
Potential disclosure and modification of persisted data	1485561	A malicious user can exploit IPM Master Data database batch data loading reports using specially crafted inputs to execute arbitrary database commands to retrieve, modify, or remove data persisted by the system. The problem is caused by an SQL injection vulnerability. The code composes an SQL statement including strings that can be altered by a malicious user. The manipulated SQL statement can then be used to retrieve additional information from the database or to potentially modify it. **Please implement the correction instructions attached to the note.**

For a list of additional security-relevant SAP Hot News and SAP Notes, see also SAP Service Marketplace at service.sap.com/securitynotes.

User Administration and Authentication

SAP Intellectual Property Management (IPM) uses the user management and authentication mechanisms of SAP NetWeaver; in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS 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 Intellectual Property Management.

SAP NetWeaver Application Server ABAP Security Guide [external document]

SAP NetWeaver Application Server Java Security Guide [external document]

User Management

Table 444

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialog user	No	Mandatory user who can access intellectual property transactions. To be maintained by an SAP CRM system administrator.
SAP NetWeaver Business Intelligence (SAP NetWeaver BI)	Personal user	No	Dialog user	No	Mandatory user who can access SAP NetWeaver BI applications. To be maintained by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	Mandatory user who can process background tasks. To be maintained by an SAP CRM system administrator.
SAP CRM	Personal or technical user	No	Dialog or system user	No	Mandatory user used for data exchange between SAP ERP and SAP CRM. Depending on whether value help is required from SAP CRM, the user type can

System	User	Delivered?	Type	Default Password	Description
					be a dialog user or system user. To be maintained by an SAP CRM system administrator.
SAP ERP	Personal or technical user	No	Dialog or system user	No	Mandatory user used for data exchange between SAP CRM and SAP ERP. Depending on the RFC destination, user can be a personal user or a system RFC user. To be maintained by an SAP ERP system administrator.

Authorizations

SAP Intellectual Property Management uses the authorization technique provided by SAP NetWeaver Application Server (SAP NetWeaver AS).

Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to SAP Intellectual Property Management.

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

SAP GUI and WebClient UI authorizations, roles, and profiles are used. The following role is in the standard system:

Table 445

Role	Description
`SAP_CRM_UIU_IPM_RIGHTSMANAGER`	PFCG Role for CRM UIU Rights Manager

Intellectual property is created using a specific product type (*Intellectual Property*) in the CRM product workbench. License contracts are created using specific business transaction types within the CRM business transaction. The following authorization objects are provided for these specific product types and business transaction types.

Table 446

Authorization Object	Description
`CRM_IPM_AV`	IPM Views for Hierarchical Attributes
`CRM_IPMCON`	CRM Order Authorization Object – Business Object License Usage Confirmation

Authorization Object	Description
CRM_IPMGRP	IPM Generation Profiles
CRM_IPMHIR	IPM Hierarchical Attributes
CRM_IPMPUC	CRM Order Authorization Object – Business Object License Acquisition Contract
CRM_IPMSAC	CRM Order Authorization Object – Business Object License Sales Contract
CRM_IPM_CC	Collision Check in License Sales Contracts
CRM_IPMRAA	IPM Rights Availability Analysis
CRM_IPMGEN	Authorization object for superordinate intellectual property in IP Mass generation
CRM_MASS	Authorization object for Mass Change Procedure

Authorization proposals are shipped for all these objects using the *Maintain the Assignments of Authorization Objects* (SU22) transaction.

Network and Communication Security

The network topology for SAP Intellectual Property Management is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* and Component-Specific Guidelines: SAP CRM [page 68] also apply to SAP Intellectual Property Management.

Communication Channel Security

The following communication channels are used:

- Remote function call (RFC)
- Business document (BDoc)
- ABAP SQL for the connection to database

Communication Destinations

Table 447

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a Web browser to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
Front-end client using SAP GUI for Windows to CRM server	Dynamic Information and Action Gateway (DIAG)	Customizing, administrative and some application data	Passwords, all sensitive CRM data such as credit card information, customer data, and conditions
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
ERP server to CRM server	RFC	System ID, client, and host name, and all application data	System information and ERP data
CRM server to BI server	RFC	System ID, client, and host name, and all application data	System information and CRM data

The following are necessary RFC authorizations for authorization object `S_RFC`:

SAP ERP to SAP CRM

Table 448

RFC Type	RFC Name	Activity
`FUGR`	`CRM_IPM_GET_IP_SEARCH_API`	`16`
`FUGR`	`BAPI_HELPVALUES_GET`	`16`
`FUGR`	`CRM_AC_ASSIGN_F4_UPLOAD`	`16`

The following are necessary authorizations in SAP ERP for transaction `JP02` (“Change Title Master”):

Table 449

Authorization Object	Description	Authorization Field Values
`M_MATE_MAF`	Material Master: Material Locks	ACTVT: 16, 51
`M_MATE_MAN`	Material Master: Data at Client Level	ACTVT: 02, 03, 06
`M_MATE_STA`	Material Master: Maintenance Statuses	ACTVT: 01,02,03,06,08 STATM: *

Additional authorization objects in SAP ERP

Table 450

Authorization Object	Description	Authorization Fields: Values
V_IPM_SD	Authorization for IP SD Product Sales	ACTVT: 01, 03
J_IPM_SD	Authorization object for SD integration of IPM project	ACTVT: 01, 03

Enterprise Services Security

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

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

Service-Oriented Architecture and Web Services

SAP Intellectual Property Management for SAP CRM 7.0 delivers three enterprise services for rights availability analysis and two services for usage confirmation.

SAP Intellectual Property Management for SAP CRM 7.0 Enhancement Pack 1 delivers four enterprise services for intellectual properties.

For security in service-oriented architecture (SOA), SAP Intellectual Property Management complies with the SOA and Web services security guidelines.

Authorization checks are implemented in proxy implementation using the existing authorization objects.

Default authorization proposals are shipped for SOA services in SAP Intellectual Property Management using *Maintain the Assignments of Authorization Objects* (transaction `SU22`).

9.10 Financial Customer Care and Dispute Management

Financial Customer Care and Dispute Management supports all financial-related communications with customers. With this scenario, the agent can access account Information, invoice/BDR information or manage disputes and adjustment requests. In addition, provider contract data from the Billing Suite (without CRM Sales and Order Management) is available directly in Financial Customer Care. The detail data of a provider contract are derived from the Common Object Layer (COL, located in the ERP system) instead of the CRM. You may need to control access to applications that display the customer personal data by restricting access only to persons who are authorized to view this information.

> Note
>
> The scenario uses the CRM Interaction Center. Therefore, the component-specific guidelines for the Interaction Center in this guide apply in addition to the information and recommendations in this section. For more information, see Component-Specific Guidelines: Interaction Center [page 202].

Technical System Landscape

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

Table 451

Topic	Guide/Tool	Quick Link SAP Service Marketplace or SDN
Technical description for *Financial Customer Care and Dispute Management* and the underlying technological components such as SAP NetWeaver	SAP for Telecommunications 2012 - Master Guide	service.sap.com/instguides

Authorizations

Access to the relevant applications can be controlled by assigning users or agents to corresponding UI profiles that either contain or do not contain the respective UI components as required.

Standard Roles

The table below shows the standard roles used by Financial Customer Care and Dispute Management.

Table 452

Business Role	PFCG Role	Description
`ETC_IC`	`SAP_CRM_UIU_ETC_IC_AGENT`	*Toll Collection IC Agent*

Business Role	PFCG Role	Description
PROVIDER_IC	SAP_CRM_UIU_PROVIDER_IC_AGENT	*Provider IC Agent*
TELCO_FCC	SAP_CRM_UIU_TELCO_FCC_AGENT	*Telco: Financial IC Agent*
TELCO_IC	SAP_CRM_UIU_TELCO_IC_AGENT	*Telco: IC Agent Master Role*
FCC_PC_ERP	SAP_CRM_UIU_FCC_PC_ERP_AGENT	Fin IC Agent – Prov Ctr in ERP

The role TELCO_IC provides access to the invoice display application (ISX_INVOICE) and the application to display event detail records (ISX_EDR) from the SAP Convergent Invoicing by default. The applications of bill display (INVOIC_S) and the billing detail records (CRM_EDR) from an external system are set as *inactive*.

A further way that you can control access to the application is by using the authorization object UIU_COMP. This object allows you to dynamically hide certain links in the navigation bar of the CRM Web UI based on the user's authorization profile.

Standard Authorization Objects

The following additional authorization objects exist:

Table 453

Authorization Object	Authorization Fields
CRM_BA_CLS	Business Agreement: Business Agreement
CRM_CMP	Authorization object CRM transaction – business transaction category: complaint (Dispute and Adjustment Request)

Table 454

Authorization Object	Authorization Fields
UIU_COMP (UIU: Component Access Authorization Check)	COMP_NAME (Component Name) COMP_WIN (Component Window Name) COMP_PLUG (Inbound Plug)

Network and Communication Security

The network topology for Financial Customer Care and Dispute Management is based on the topology used by the SAP NetWeaver platform and middleware in SAP CRM. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to this scenario. For more information, see the main Network and Communication Security [page 29] section in this guide.

Communication Destinations

In addition to the general paths used by SAP CRM, the Financial Customer Care and Dispute Management scenario also uses the following communication path:

Table 455

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to ERP server	RFC	System ID, client, and host name, and all application data	System information and CRM data

The connection from SAP CRM to SAP ERP should be configured as a trusted system to grant a higher security level. We recommend that you use named users, that means, Contract Accounts Receivable and Payable (FI-CA) and CRM use the same user names. For ERP-related objects the authority checks can only be processed in the ERP-system. Therefore the ERP user needs the relevant authorizations.

Data Storage Security

In processes that involve capturing refill requests, credit card data is displayed and captured. This data is technically stored along with other credit cards in the *Account* master data object (see Data Storage Security [page 33]).

For more information about how to enable encryption, see section Payment Card Security According to PCI-DSS [page 42].

Other Security-Relevant Information

Since the Financial Customer Care and Dispute Management scenario uses both the Interaction Center WebClient in SAP CRM and Contract Accounts Receivables and Payables (FI-CA) in SAP ERP, the corresponding security guides for these also apply. You should, therefore, also take into account any security-related recommendations or specific restrictions indicated in the following security guides:

- See SAP Library for SAP ERP Central Component on SAP Help Portal at help.sap.com/ecc > *<Choose relevant release>* > *Application Help* : Search for *Contract Accounts Receivable and Payable (FI-CA) Security Guide*
- See SAP Library for SAP ERP Central Component on SAP Help Portal at help.sap.com/ecc > *<Choose relevant release>* > *Application Help* : Search for *SAP ECC Industry Extension Telecommunications Security Guide*

9.11 Utilities: B2C Call Center and B2B Work Center

The SAP Customer Relationship Management and Billing for Utilities package supports business-to-consumer (B2C) and business-to-business (B2B) contract management for residential and industrial customers.

For residential customers, processes such as selling energy products, changing budget billing plans, entering meter reading results, starting market communication, correcting bills, and changing master data are offered.

For industrial customers, additional processes are available, such as collecting points of delivery for individual price calculation, master agreement, and energy profile management.

Authorizations

In SAP for Utilities, the following additional authorization objects exist:

Table 456

Authorization Object	Description
CRM_ISUITY	Authorization Object for Processing of Item Categories
CRM_ISUPRF	Authorization Object for Processing Profiles
CRM_BA_CLS	Business Agreement: Business Agreement Class
CRM_IUDISI	Utilities Disconnect/Reconnect Immediately
CRM_IUPROC	Auth. obj - IS-U Process Execution

Data Protection

To complete utilities objects (such as contracts and quotations) before enabling the end of purpose check function for the central business partner, run the report `ECRM_ISU_ORDER_DPP_COMPLETE`. If you want to add company-specific settings, you can create your own report and use this one as a template. For more information, see the Data Protection [page 35] section.

9.12 Utilities: Demand Side Management

Demand side management (DSM) refers to the management of energy demand by influencing the quantity of consumed energy (energy efficiency) or the patterns of energy use (demand response). It aims to promote energy efficiency, optimize generation resources, and safeguard grid operation. In addition, it aims to optimize the procurement of energy.

The SAP Demand Side Management solution (SAP DSM) enables you to define energy efficiency and demand response programs, measures and incentives, create and review applications for programs, manage agreements, process incentives (using the FI-CA component of SAP ERP), and monitor and analyze program performance.

Fundamental Security Guides

SAP DSM is a utility industries-specific solution managed using SAP Customer Relationship Management (SAP CRM). As such, all of the security information specified in Chapter 1 of this guide is also applicable to SAP Demand Side Management.

Any additional information specific to SAP DSM is provided in the sections below.

Technical System Landscape

SAP DSM is primarily based on SAP CRM. For more information, see Technical System Landscape [page 9].

Of all the systems included as part of the SAP CRM technical system landscape, SAP Enterprise Resource Planning (SAP ERP) and SAP NetWeaver Business Warehouse can be included in the landscape for SAP DSM when tasks such as incentive processing and program monitoring and analysis are required.

User Management

User Types

For more information on the user types required for SAP CRM, see User Management [page 18].

For SAP DSM, the user type that is required is the *dialog user created using the User Maintenance transaction (individual user)*, used to carry out functions in SAP GUI and in the WebClient UI.

Standard Users

No standard users are provided.

Authorizations

Standard Roles

The table below shows the standard roles that are used by SAP DSM.

Table 457

Business Role	PFCG Role
UTIL_DSM_MGR (Utilities DSM Program Manager)	SAP_CRM_UIU_UTIL_DSM_PROG_MGR (DSM Program manager)
UTIL_DSM_INP (Utilities DSM Inspector)	SAP_CRM_UIU_SRV_PROFESSIONAL (Service Professional)

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP DSM.

Table 458

Authorization Object	Field	Value	Description
CRM_DSMPRG	ACTVT	01, 02, 03, 05, 06, 24, 43, 70, 95, D9	Permitted activities related to program management Note In order to have authorization to create or delete a program, you need to have authorization to edit the program.
	CRM_DSM_AG	-	Program's authorization group to which the associated user role has access
CRM_DSMAPL	ACTVT	45	Authorization to process applications
CRM_DSMAGR	ACTVT	45	Authorization to process agreements
CRMDSMAPLS	ACTVT	01, 02, 03, 06, 43, 96, D5, D6, D7, D8, DG, DI, DR	Permitted activities related to application processing
	CRM_DSM_AG	-	Program's authorization group to which the associated user role has access
CRMDSMAGRS	ACTVT	01, 02, 03, 06, 43, 96, D4, D5, D6, D8, D9, DG, DI, DR	Permitted activities related to agreement processing

Authorization Object	Field	Value	Description
	CRM_DSM_AG	-	Program's authorization group to which the associated user role has access

Necessary RFC Authorizations for Authorization Object S_RFC (CRM to ERP)

Table 459

Authorization Object	Field	Value	Description
S_RFC	RFC_TYPE	FUGR	The type of RFC to protect; in this case, the value corresponds to "Function group"
	RFC_NAME	FKK_CRM_XBILL_ONEOFF_INBOUND	The name of the RFC object to protect
	ACTVT	16	The activity value corresponds to "Execute"

Necessary Authorizations in SAP ERP

SAP DSM uses the SAP Convergent Invoicing feature in SAP ERP during agreement processing. Therefore the security recommendations and guidelines for authorizations as described in the security guide for SAP Contract Accounts Receivable and Payable (FI-CA) Security Guide also apply for SAP DSM.

For more information, see Contract Accounts Receivable and Payable (FI-CA) Security Guide on SAP Service Marketplace (service.sap.com/securityguide).

Network and Communication Security

Communication Channel Security

For more information on communication channel security used by SAP CRM, see Network and Communication Security [page 29].

SAP DSM uses the following communication paths:

Table 460

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
CRM server to ERP server	RFC	System ID, client, host name and all application data	System information and CRM data
CRM server to business intelligence (BI) server	RFC	System ID, client, host name and all application data	System information and CRM data
WebClient UI to CRM server	HTTP/HTTPS	All application data	Passwords, all sensitive CRM data

Security-Relevant Logging and Tracing

You need to ensure that the following check is made on newly-created tables:

All the transparent tables of Data Class 'APPL2' (Organization and Customizing) should have the 'Log Data Changes' checked in the Technical Settings.

If you have created transparent tables for Organization and Customizing, perform the following check.

- In transaction SE11, display the table and select the *Technical Settings* button.
- If in the Logical Storage parameters, the table has the Data class APPL2 assigned, select the *Log Data Changes* checkbox

Note

The *Log Data Changes* check box should only be enabled for the APPL2 tables.

For more information on security-relevant logging and tracing used by SAP CRM, see Trace and Log Files [page 54].

9.13 Waste and Recycling

The waste and recycling application in SAP CRM is part of SAP for Utilities and represents a new user interface for the selected functions of SAP Waste and Recycling of SAP enhancement package 5 for SAP ERP.

The interaction center agent is able control the all aspects of the container service: account management (CRM standard, replicated data from CRM to ERP, and vice versa), container management (allocating, placing, removing) and the whole contract handling for container management. It is possible to see all information from different views: customer view, from service address and from object address.

Related Security Guides

This CRM UI is not a standalone application; there has to be a connection to the ERP system. In this case, all security aspects given here are directly connected to the security guide for SAP Waste and Recycling at service.sap.com/securityguide.

Technical System Landscape

In order to use the waste and recycling application in SAP CRM, there has to be a connected ERP system (minimum enhancement package 5 for SAP ERP, with SAP Waste and Recycling included). The waste and recyling application cannot run in SAP CRM on its own. In other words, it is a UI for selected ERP functions of SAP Waste and Recycling.

The connection between both systems is handled by the SAP RFC connector, which uses the default IS-U RFC destination. All method calls from CRM will be converted into data blocks, transmitted to the receiver part of the RFC connector, which transforms it back to the method call. The results are returned the same way. The SAP RFC connector parts are shipped in CRM 7.01 and enhancement package 5 for SAP ERP with SAP Waste and Recycling.

User Administration and Authentication

The waste and recycling application in SAP CRM uses the user management and authentication mechanisms of SAP NetWeaver; in particular, the security features of SAP NetWeaver Application Server ABAP (SAP NetWeaver AS ABAP). Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide*, available at help.sap.com/nw_platform also apply to this module.

User Management

Table 461

System	User	Delivered?	Type	Default Password	Description
SAP Customer Relationship Management (SAP CRM)	Personal user	No	Dialog user	No	Mandatory to act as an interaction center agent. To be maintained by an SAP CRM system administrator.
SAP ERP	Personal user	No	Dialog user	No	Mandatory to act as an interaction center agent in CRM. Note: This is just for trusted system-configured RFC destinations in CRM. Otherwise it is not necessary. To be maintained by an SAP ERP system administrator.
SAP CRM	Personal or technical user	No	Dialog or system user	No	Mandatory user is used to customize data exchange between SAP CRM and SAP ERP (transaction SPRO). This can be done by the CRM administrator, too. To be maintained by an SAP CRM system administrator.
SAP CRM	Technical user	No	System user	No	If trusted system is not configured in an RFC destination in CRM, remote user has to be created for RFC calls to the back-end ERP system. To be maintained by an SAP CRM

System	User	Delivered?	Type	Default Password	Description
					system administrator.
SAP ERP	Technical user	No	System user	No	If trusted system is not configured in an RFC destination of CRM, remote user has to be created for RFC calls from CRM. To be maintained by an SAP CRM system administrator.

To use the SAP RFC connector, the RFC calling user (depending on whether a trusted system is used or not) requires at least the following authorizations for authorization object S_RFC:

Table 462

RFC_TYPE	RFC_NAME	ACTVT
FUGR	EEWA_CONNECTOR_BASE	16

Authorizations

The following table shows the standard roles that are used by the waste and recycling application in SAP CRM:

Table 463

Role	Description
SAP_CRM_UIU_EWA_IC_AGENT	This standard role is delivered using the WebClient UI (used by business role EWA_IC_AGENT).

Network and Communication Security

All data and functions are stored in ERP, so there has to be a RFC destination. This destination is provided by IS-U standard but can be overwritten using Customizing. The connection from CRM to ERP should be configured as a trusted system to grant a higher security level by calling methods in the ERP system. If no trusted connection is customized, a background user in the ERP system must be created, which is set in the RFC destination of SAP CRM (see the *User Management* section).

A connection from ERP to SAP CRM is not necessary.

9.14 Service Parts Management: OEM-Managed Inventory with SAP CRM Sales Orders

You can create sales orders in SAP Customer Relationship Management (SAP CRM) as part of the inventory process managed by the original equipment manufacturer (OEM) within service parts management. The OEM-managed inventory process allows OEM to plan stocks for dealers or customers. Once a replenishment order is approved in SAP Supply Chain Management (SAP SCM), the system creates a sales order in either SAP ERP or in SAP CRM.

In addition to the function-specific security aspects outlined in this security guide section, the security aspects in the Quotation and Order Management [page 150] section also apply.

Related Security Guides

OEM-managed inventory with SAP CRM sales orders belongs to service parts management in SAP Service and Asset Management. The security guide for SAP Service and Asset Management also applies to OEM-managed inventory with SAP CRM sales orders. For more information, see SAP Service Marketplace at service.sap.com/securityguide > *Industry Solutions* > *SAP Service and Asset Management* > *SAP Service and Asset Management: Scenario Security Guide*.

For a complete list of the available SAP security guides, see SAP Service Marketplace at service.sap.com/securityguide.

Important SAP Notes

The SAP Notes that apply to quotation and order management also apply to OEM-managed inventory with CRM sales orders.

Technical System Landscape

For more information about the technical system landscape, see the references listed in the following table:

Table 464

Topic	Document	Document Location
Technical description of the scenarios in SAP Service and Asset Management and the underlying technological components such as SAP NetWeaver	Master guide for *SAP Service and Asset Management*	service.sap.com/instguides > *Industry Solutions* > *Industry Solution Guides* > *SAP Service and Asset Management*
Security	See applicable documents	sdn.sap.com/irj/sdn/security

Security Aspects of Data, Data Flow and Processes

The figure below shows an overview of the data flow for OEM-managed inventory with SAP CRM sales orders in service parts management:

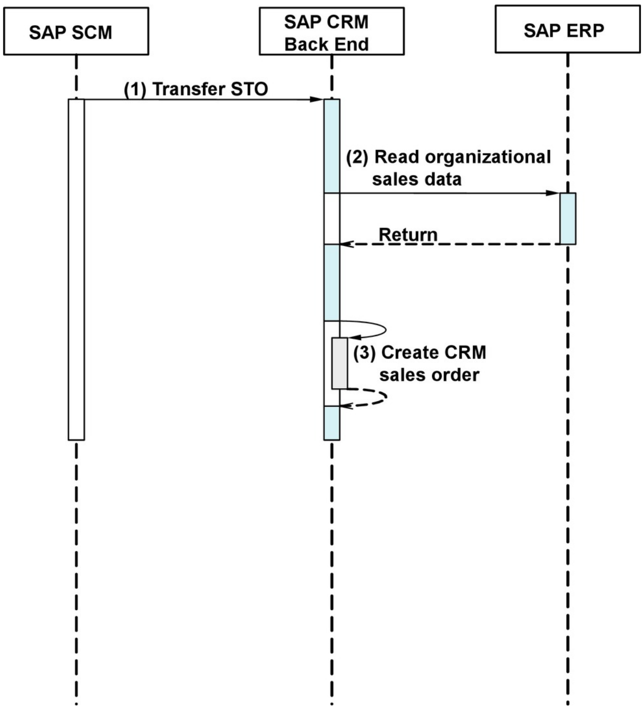

SAP SCM
SAP CRM Back End
SAP ERP
(1) Transfer STO
(2) Read organizational sales data
Return
(3) Create CRM sales order

Figure 37: Overview of Process Steps for OEM-Managed Inventory with SAP CRM Sales Orders

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

Table 465

Step	Description	Security Measure
1	Transfer stock transport order (STO) Approved STOs are transferred to the SAP CRM back-end system (asynchronous RFC-based communication).	Mandatory user used for data exchange between SAP SCM and SAP CRM
2	Read organizational sales data Read the sales areas to which the location is mapped in Customizing for SAP ERP (synchronous RFC-based communication).	User who can process background jobs
3	Create CRM sales order	Not applicable

User Administration and Authentication

OEM-managed inventory with SAP CRM sales orders uses the user management and authentication mechanisms provided with the SAP NetWeaver Application Server (AS) ABAP. The security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to OEM-managed inventory with SAP CRM sales orders.

User Management

User management for OEM-managed inventory with SAP CRM sales orders uses the mechanisms provided with the SAP NetWeaver Application Server, for example, tools, user types, and password policies.

User Management Tools

The following table shows the relevant tools for user management and user administration for OEM-managed inventory with SAP CRM sales orders:

Table 466

Tools	Description
User and role administration with SAP NetWeaver Application Server ABAP: User maintenance (transaction `SU01`) and profile generator (transaction `PFCG`)	For more information, see the User Management [page 18] section.

User Types

The following table shows the required technical user types:

Table 467

User Type	Description
Communication user	For the transfer of STOs from a connected SAP SCM system
Background user	For processing the transferred STOs to create CRM sales orders

For information about the user types above, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw_platform › *<Choose relevant release>* › *Security Information* › *Security Guide* › *Security Guides for SAP NetWeaver Functional Units* › *Security Guides for the Application Server* › *Security Guides for the AS ABAP* › *SAP NetWeaver Application Server ABAP Security Guide* › *User Administration and Authentication* › *User Management* ›.

The following table shows the users that must be created for operating OEM-managed inventory with SAP CRM sales orders:

Table 468

System	User	Delivered	Type	Default Password	Description
SAP SCM	All users	No	System user	No	Mandatory user for data exchange between SAP SCM and SAP CRM
SAP CRM	All users	No	System user or dialog user	No	Mandatory user who can process background jobs

For information about the required users for processing SAP CRM sales orders, see the Quotation and Order Management [page 150] section.

Authorizations

OEM-managed inventory with SAP CRM sales orders uses the authorization concept provided by SAP NetWeaver AS ABAP. The recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to OEM-managed inventory with SAP CRM sales orders. For more information, see the Authorizations [page 25] section.

Network and Communication Security

The network topology for OEM-managed inventory with SAP CRM sales orders is based on the network topology used by the SAP NetWeaver platform. The security guidelines and recommendations described in the *SAP*

NetWeaver Security Guide also apply to OEM-managed inventory with SAP CRM sales orders. For more information, see the Network and Communication Security [page 29] section.

Communication Channel Security

The following table shows the communication channels used by OEM-managed inventory with SAP CRM sales orders, the protocol used for the connection, and the type of data transferred:

Table 469

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
SCM server to CRM server	RFC	• System ID • Client and host name • STO data	• System information • SCM STO data
CRM server to ERP server	RFC	• System ID • Client • Sales area in Customizing entries for location	System information

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

Communication Destinations

The following table shows the communication destinations used by OEM-managed inventory with SAP CRM sales orders:

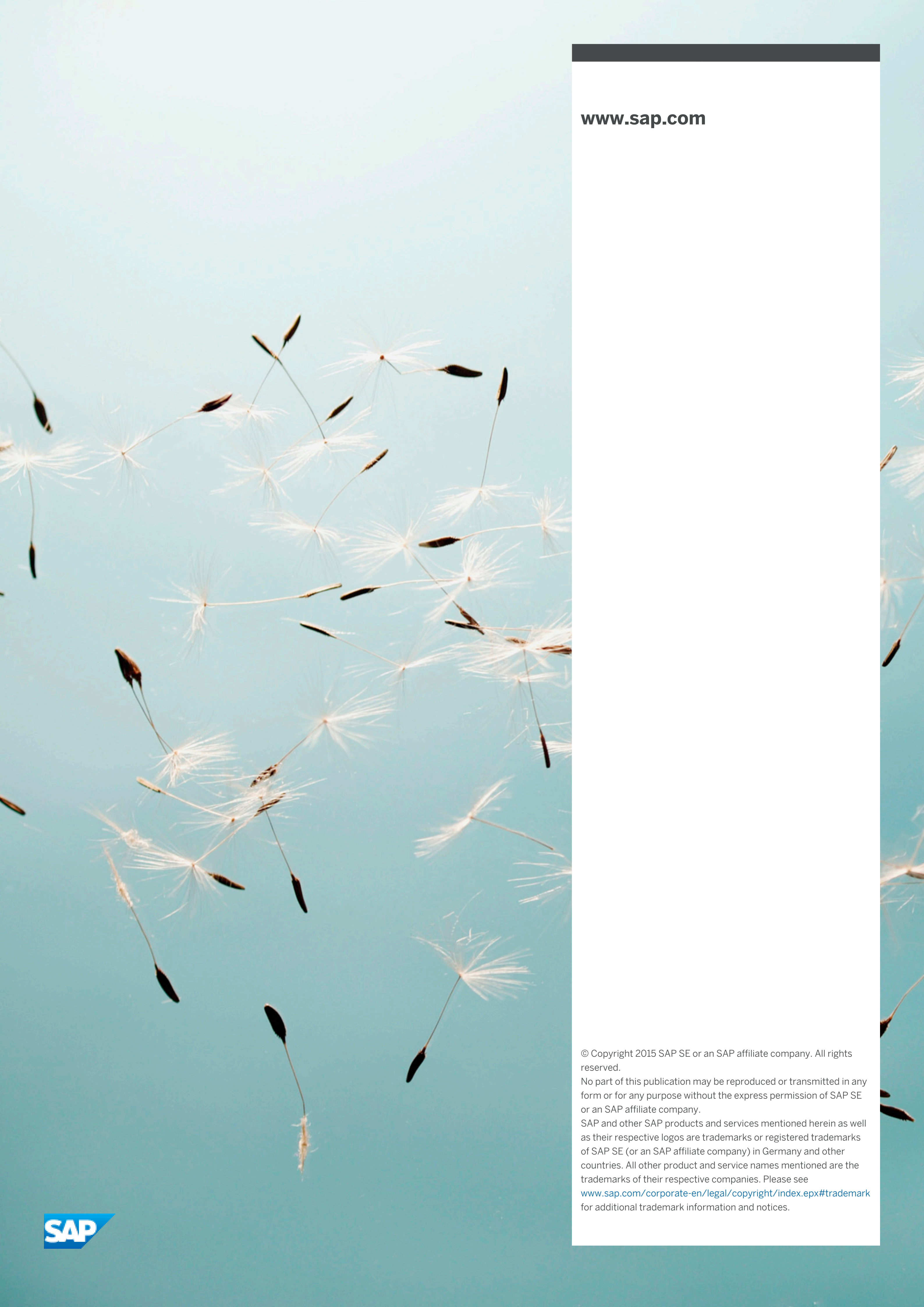
Table 470

Destination	Delivered	Type	User and Authorizations	Description
SAP CRM	No	RFC	Not delivered	Connection from SAP SCM to SAP CRM for data exchange
SAP ERP	No	RFC	Not delivered	Connection from SAP CRM to SAP ERP to read the sales areas to which the location is mapped in Customizing for SAP ERP

Typographic Conventions

Table 471

Example	Description
<Example>	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your **<User Name>**”.
▶ *Example* ▶ *Example* ▶	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
Example	Words or characters that you enter in the system exactly as they appear in the documentation
www.sap.com	Textual cross-references to an internet address
/example	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
123456	Hyperlink to an SAP Note, for example, SAP Note 123456
Example	• Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. • Cross-references to other documentation or published works
Example	• Output on the screen following a user action, for example, messages • Source code or syntax quoted directly from a program • File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE
EXAMPLE	Keys on the keyboard



www.sap.com