Copyright

© Copyright 2004 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

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

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

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

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

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

Java is a registered trademark of Sun Microsystems, Inc.

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

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.
Icons in Body Text

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Caution</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Example</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Note</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Recommendation</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Syntax</td>
</tr>
</tbody>
</table>

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

Typographic Conventions

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example text</em></td>
<td>Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Emphasized words or phrases in body text, graphic titles, and table titles.</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td><em>&lt;Example text&gt;</em></td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Keys on the keyboard, for example, F2 or ENTER.</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Security Guide for mySAP CRM</td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Before you start</td>
<td>11</td>
</tr>
<tr>
<td>mySAP CRM Key Capabilities Overview</td>
<td>13</td>
</tr>
<tr>
<td>Technical System Landscape</td>
<td>15</td>
</tr>
<tr>
<td>User Management and Authentication</td>
<td>23</td>
</tr>
<tr>
<td>User Management</td>
<td>25</td>
</tr>
<tr>
<td>User Data Synchronization</td>
<td>34</td>
</tr>
<tr>
<td>Integration with the Single Sign-On Environment</td>
<td>35</td>
</tr>
<tr>
<td>Authorizations</td>
<td>37</td>
</tr>
<tr>
<td>Network and Communication Security</td>
<td>39</td>
</tr>
<tr>
<td>Communication Channel Security</td>
<td>40</td>
</tr>
<tr>
<td>Network Security</td>
<td>42</td>
</tr>
<tr>
<td>Communication Destinations</td>
<td>44</td>
</tr>
<tr>
<td>Data Synchronization</td>
<td>45</td>
</tr>
<tr>
<td>User Data Synchronization</td>
<td>46</td>
</tr>
<tr>
<td>Data Storage Security</td>
<td>47</td>
</tr>
<tr>
<td>Security for Third-Party or Additional Applications</td>
<td>49</td>
</tr>
<tr>
<td>Dispersable Functions with Impacts on Security</td>
<td>50</td>
</tr>
<tr>
<td>Other Security-relevant Information</td>
<td>51</td>
</tr>
<tr>
<td>Trace and Log Files</td>
<td>53</td>
</tr>
<tr>
<td>CRM Component Specific Security Guidelines</td>
<td>54</td>
</tr>
<tr>
<td>CRM Enterprise</td>
<td>55</td>
</tr>
<tr>
<td>Enterprise Sales</td>
<td>58</td>
</tr>
<tr>
<td>Enterprise Service and Analytics</td>
<td>64</td>
</tr>
<tr>
<td>Enterprise Marketing</td>
<td>67</td>
</tr>
<tr>
<td>Product Proposals</td>
<td>68</td>
</tr>
<tr>
<td>External List Management</td>
<td>70</td>
</tr>
<tr>
<td>Segment Builder</td>
<td>73</td>
</tr>
<tr>
<td>Digital Asset Management</td>
<td>75</td>
</tr>
<tr>
<td>Campaign Management</td>
<td>80</td>
</tr>
<tr>
<td>Field Applications</td>
<td>83</td>
</tr>
<tr>
<td>Mobile Sales</td>
<td>84</td>
</tr>
<tr>
<td>Hard Drive Encryption</td>
<td>88</td>
</tr>
<tr>
<td>Mobile Service</td>
<td>94</td>
</tr>
<tr>
<td>Mobile Client Synchronization</td>
<td>95</td>
</tr>
<tr>
<td>Mobile Sales and Service for Handheld Using CRM</td>
<td>104</td>
</tr>
<tr>
<td>SAP E-Commerce</td>
<td>107</td>
</tr>
<tr>
<td>E-Service</td>
<td>134</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>Payment Cards Encryption</td>
<td>140</td>
</tr>
<tr>
<td>Selling via eBay</td>
<td>144</td>
</tr>
<tr>
<td>SAP Internet Pricing and Configurator</td>
<td>151</td>
</tr>
<tr>
<td>Interaction Center</td>
<td>156</td>
</tr>
<tr>
<td>Interaction Center WinClient</td>
<td>157</td>
</tr>
<tr>
<td>Interaction Center WebClient</td>
<td>163</td>
</tr>
<tr>
<td>E-Mail Response Management System</td>
<td>173</td>
</tr>
<tr>
<td>Interaction Center Manager</td>
<td>179</td>
</tr>
<tr>
<td>Interaction Center: Workforce Management Services</td>
<td>184</td>
</tr>
<tr>
<td>Channel Management</td>
<td>189</td>
</tr>
<tr>
<td>Channel Sales Management for High-Tech</td>
<td>193</td>
</tr>
<tr>
<td>Contracts and Chargeback for Pharmaceutical</td>
<td>198</td>
</tr>
<tr>
<td>Lead Management with Channel Management</td>
<td>203</td>
</tr>
<tr>
<td>CRM Billing</td>
<td>205</td>
</tr>
<tr>
<td>CRM Rebates</td>
<td>210</td>
</tr>
<tr>
<td>SAP CRM Powered by SAP NetWeaver</td>
<td>214</td>
</tr>
<tr>
<td>CRM Server</td>
<td>215</td>
</tr>
<tr>
<td>Software Agent Framework</td>
<td>221</td>
</tr>
<tr>
<td>Solution Database</td>
<td>224</td>
</tr>
<tr>
<td>People-Centric User Interface</td>
<td>226</td>
</tr>
<tr>
<td>Calendar (ActiveX) Control</td>
<td>231</td>
</tr>
<tr>
<td>SAP Business Information Warehouse</td>
<td>233</td>
</tr>
<tr>
<td>Object Links, Input Help, Core Services, and Java Lists</td>
<td>234</td>
</tr>
<tr>
<td>BSP Application</td>
<td>237</td>
</tr>
<tr>
<td>CRM Access Control Engine</td>
<td>238</td>
</tr>
<tr>
<td>Knowledge Management</td>
<td>241</td>
</tr>
<tr>
<td>Alerts</td>
<td>244</td>
</tr>
<tr>
<td>Roles in the ABAP System for Portal Users</td>
<td>246</td>
</tr>
<tr>
<td>Portal Telephony Integration</td>
<td>249</td>
</tr>
<tr>
<td>Industry-Specific CRM</td>
<td>250</td>
</tr>
<tr>
<td>Account Origination</td>
<td>251</td>
</tr>
<tr>
<td>SAP Leasing</td>
<td>253</td>
</tr>
<tr>
<td>Media: Intellectual Property Management (IPM)</td>
<td>255</td>
</tr>
<tr>
<td>Telco Dealer Application</td>
<td>256</td>
</tr>
<tr>
<td>Master Data</td>
<td>257</td>
</tr>
<tr>
<td>CRM Price List</td>
<td>258</td>
</tr>
<tr>
<td>Appendix</td>
<td>262</td>
</tr>
</tbody>
</table>
Security Guide for mySAP CRM

In the following you will find security guidelines with respect to SAP Customer Relationship Management (CRM).
Introduction

This guide does not replace the Daily Operations Handbook, which we recommend you use to create your specific productive operations.

You find the current version of the security guide on the SAP Service Marketplace under service.sap.com/securityguide → SAP Customer Relationship Management (CRM) Security Guides.

Target audience

- Technology consultants
- System administrators

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

Why is Security necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to mySAP CRM since important business data and personal information are processed and stored by mySAP CRM.

mySAP CRM enables you to collaborate with your in-house and field employees, and with your partners and customers. Therefore, the components of mySAP CRM will access multiple data sources and business processes on behalf of different users holding different roles and thus requiring different level of security. To meet your business needs, mySAP CRM allows to make use of various access possibilities involving several technical mechanisms.

In general, access to the data available within mySAP CRM must only be granted to authorized users. Unfortunately, no unique and uniform security implementation exists that would fit to all possible usage scenarios. Therefore, mySAP CRM provides you with flexible and configurable security mechanisms, which allow you to implement the necessary security restrictions according to your security requirements.

For example, mySAP 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 such as:
  - 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 also section “Technical System Landscape”) the information must be protected on different levels and using different protection mechanisms. Note, that
the information is not only available by using the application features of mySAP CRM functions but may also be visible at technical levels (e. g. the network) if not appropriately secured.

⚠️

To show the importance of correct security configuration consider the following attack scenarios when using any CRM solution:

- Due to a misconfiguration in the access restrictions an administrative interface can be accessed from the Internet. Attackers have managed to recognize the weakness and after appropriate changes using the administration functions are able to access data of other users.

- A laptop of a mobile sales representative has been stolen. Unfortunately the local information store holding your CRM information has not been secured and contains all information about your offer concerning a large volume contract for which your company is competing with several other companies. Because the information is brought to the attention of your strongest competitor he adjusts his offer appropriately and wins the contract.

These few attack scenarios show that in general protecting your data by appropriate security configuration can be crucial for your business success. To assist you in securing mySAP CRM, we provide this Security Guide.

About this document

The Security Guide provides an overview of the security-relevant information that applies to mySAP CRM. Since mySAP CRM consists of several components, this document first contains an overview with general security recommendations applying uniformly to mySAP CRM. Then individual security guidelines for each of the underlying components are given.

💡 Note, that some mySAP CRM components use different or additional concepts and mechanisms with respect to the topics (e. g. authorization or data storage security) described in the main sections of this Security Guide. The deviations and related configuration is described in the component specific part of this guide. Therefore it is necessary to read both the general and the relevant component specific part of this Security Guide.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- Introduction
  The section you are currently reading. It contains information about the target audience, explains why security is necessary, and gives an overview of the main sections of this Security Guide.

- **Before You Start** [Seite 11]
  This section contains information about how to use this document, lists important SAP Notes for mySAP CRM and references to other Security Guides that build the foundation for this Security Guide.

- **Technical System Landscape** [Seite 15]
This section provides an overview of the technical components and communication paths that are used by mySAP CRM. Several typical mySAP CRM use scenarios are shown with its relevant components and its specific security requirements.

- **User Management and Authentication [Seite 23]**
  This section provides an overview of the following user administration and authentication aspects:
  - Recommended tools to use for user management.
  - User types that are required by mySAP CRM.
  - Standard users that are delivered with mySAP CRM.
  - Overview of the user synchronization strategy, if several components or products are involved.
  - Overview of how integration into Single Sign-On environments is possible.

- **Authorizations [Seite 37]**
  This section provides an overview of the overall authorization concepts that applies to mySAP CRM in general.

- **Network and Communication Security [Seite 39]**
  This section provides an overview of the communication paths used by mySAP CRM and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- **Data Storage Security [Seite 47]**
  This section provides an overview of any critical data that is used by mySAP CRM and the security mechanisms that apply.

- **Security for Third-Party or Additional Applications [Seite 49]**
  This section provides security information that applies to third-party or additional applications that are used with mySAP CRM.

- **Dispensable Functions with Impacts on Security [Seite 50]**
  This section provides an overview of functions that have impacts on security and can be disabled or removed from the system.

- **Other Security-Relevant Information [Seite 51]**
  This section contains information about additional security-relevant tasks.

- **Trace and Log Files [Seite 53]**
  This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

- **CRM Component Specific Guidelines [Seite 54]**
  This section provides security related information specific for the different mySAP CRM components. The information is structured according to the mySAP CRM key capabilities:
  - CRM Enterprise
  - Field Applications
  - E-Commerce
  - Interaction Center
You will need to read both the general sections and the relevant component specific sections.

- **Appendix [Seite 262]**
  
  This section provides references to further information.
**Before you start**

**Fundamental Security Guides**

mySAP CRM is build on top of several standard SAP components. Therefore, the corresponding Security Guides also apply to mySAP CRM. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

**Fundamental Security Guides**

<table>
<thead>
<tr>
<th>Scenario, Application or Component</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebAS Java (part of NetWeaver)</td>
<td></td>
</tr>
<tr>
<td>SAP Enterprise Portal 5.0</td>
<td></td>
</tr>
<tr>
<td>SAP Enterprise Portal 6.0</td>
<td></td>
</tr>
<tr>
<td>SAP Content Server</td>
<td></td>
</tr>
<tr>
<td>SAP TREX</td>
<td></td>
</tr>
<tr>
<td>SAP BW</td>
<td></td>
</tr>
<tr>
<td>SAP APO</td>
<td></td>
</tr>
<tr>
<td>SAP FSCM-Biller Direct</td>
<td></td>
</tr>
<tr>
<td>SAP Mobile Infrastructure</td>
<td></td>
</tr>
<tr>
<td>SAP Business Connector</td>
<td></td>
</tr>
<tr>
<td>SAP Credit Management Server</td>
<td></td>
</tr>
<tr>
<td>SAP Guided Selling</td>
<td></td>
</tr>
<tr>
<td>SAP Multichannel Interface Server</td>
<td></td>
</tr>
<tr>
<td>SAP Broadcast Messaging Server</td>
<td></td>
</tr>
</tbody>
</table>

You will find a complete list of the available SAP Security Guides on the SAP Service Marketplace under [service.sap.com/securityguide](http://service.sap.com/securityguide).

**Important SAP Notes**

The most important SAP Notes that apply to the security of mySAP CRM are shown in the table below.

**Important SAP Notes**

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>754723</td>
<td>SAP CRM 4.0 SR01 Release and Information Note</td>
<td>Important note about available patch levels for mySAP CRM components</td>
</tr>
<tr>
<td>604746</td>
<td>SAP CRM 4.0: Information about Installation</td>
<td></td>
</tr>
<tr>
<td>604728</td>
<td>SAP CRM 4.0: Information on Upgrade</td>
<td></td>
</tr>
<tr>
<td>543841</td>
<td>CRM Support Packages</td>
<td></td>
</tr>
<tr>
<td>Collective Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>605798 Installation Guide – SAP CRM / SRM 4.0 Server on Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>605799 Installation Guide – SAP CRM / SRM 4.0 Server on Unix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>632030 Additions to Solution Upgrade Guide mySAP CRM 4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>715371 SAP J2EE - Sammelhinweis Sicherheit Basis 6.30/6.40 A very important note to use the J2EE Engine Basis 6.30 and 6.40 on a secure way</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additional Information**

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

**Quick Links to Additional Information**

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on the SAP Service Marketplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>mySAP CRM</td>
<td>service.sap.com/crm</td>
</tr>
<tr>
<td>mySAP CRM Best Practices</td>
<td>service.sap.com/bp-crm</td>
</tr>
<tr>
<td>mySAP CRM Installation and Upgrade</td>
<td>service.sap.com/crm-inst</td>
</tr>
<tr>
<td>mySAP CRM Solution Library</td>
<td>service.sap.com/crm-solution</td>
</tr>
<tr>
<td>mySAP CRM Integration Services (also known as CRM Middleware)</td>
<td>service.sap.com/crm-mw</td>
</tr>
<tr>
<td>Security</td>
<td>service.sap.com/security</td>
</tr>
<tr>
<td>Security Guides</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td>service.sap.com/notesc</td>
</tr>
<tr>
<td>Released platforms</td>
<td>service.sap.com/platforms</td>
</tr>
<tr>
<td>Network security</td>
<td>service.sap.com/network</td>
</tr>
<tr>
<td>Technical infrastructure</td>
<td>service.sap.com/ti</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>service.sap.com/solutionmanager</td>
</tr>
</tbody>
</table>
mySAP CRM Key Capabilities Overview

mySAP CRM provides a set of key capabilities each tailored to provide you with the best support for the different CRM requirements. Each key capability can therefore be used in dedicated CRM scenarios and may also provide special support functions.

The following list provides you with an overview on the mySAP CRM key capability structure using the following pattern:

**Key Capability**
- System Landscape

**CRM Enterprise**
- Enterprise Sales
  - Sales Planning and Forecasting
- Enterprise Service and Analytics
- Enterprise Marketing
  - Product Proposals
  - External List Management

**Field Applications**
- Mobile Sales
- Mobile Service
- Mobile Client Synchronization
- Mobile Sales and Service for Handheld Using CRM 4.0

**E-Commerce**
- E-Service
- SAP Internet Sales
- Selling Via eBay

**Interaction Center**
- Interaction Center WinClient
- Interaction Center WebClient
- E-Mail Response Management System
- Interaction Center Manager
- Interaction Center: Workforce Management Services

**Channel Management**
- Channel Sales Management for High Tech
- Contracts and Chargeback for Pharmaceutical
SAP CRM Powered by SAP NetWeaver

- CRM Server
- Software Agent Framework
- Solution Database
- CRM Billing
- Intelligence Connector
- SAP Internet Pricing and Configurator
- People-Centric CRM
  - People-Centric User Interface
- SAP Business Information Warehouse
- Objektlinks, Wertehilfe, Core Services und Java-Listen
- SAP Internet Sales
- BSP-Applikation
- CRM-Access-Control-Engine
- Knowledge Management
- Alerts
- Integration der SAP R/3-Transaktionen in Portalrollen
- Rollen im CRM-System für Portalbenutzer

For more information about the functions, installation, and operation of the mySAP CRM key capabilities please refer to the mySAP CRM information at the SAP Service Marketplace under service.sap.com/crm and the documentation at the SAP Help Portal under help.sap.com → Documentation → mySAP Business Suite → mySAP Customer Relationship Management.
**Technical System Landscape**

Security does not only depend on sound configuration of each of the mySAP CRM components, it also depends on the technical system landscape. The technical system landscape is concerned with several topics, such as:

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

The figure below shows a general overview of the maximal technical system landscape for mySAP CRM.

![Diagram of the technical system landscape for mySAP CRM](image)

Normally you will only install specific parts of this mySAP CRM system landscape depending on the functionality necessary to fulfill your business needs.

![Note](image)

Note, that there is no single typical system landscape for mySAP CRM. Since the system landscape depends on the mySAP CRM use scenario there are several typical system landscape layouts according to the key capabilities required for a mySAP CRM system installation.

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

![We recommend performing a sound security analysis and evaluation](image)

We recommend performing a sound security analysis and evaluation for a new or modified system landscape with all its components. Normally it makes sense...
to acquire external support (e. g. your own company's security team or an external service provider) for security related consulting or to perform the security assessment.

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

### More Information About the Technical System Landscape

<table>
<thead>
<tr>
<th>Topic</th>
<th>Guide/Tool</th>
<th>Quick Link to the SAP Service Marketplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical description for mySAP CRM and the underlying technological components such as SAP NetWeaver</td>
<td>Master Guide</td>
<td>service.sap.com/instguides</td>
</tr>
<tr>
<td>Technical configuration</td>
<td>Technical Infrastructure Guide</td>
<td>service.sap.com/ti</td>
</tr>
<tr>
<td>High availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td>service.sap.com/security</td>
</tr>
</tbody>
</table>

### Security Dependency: mySAP CRM and Base Components

mySAP CRM is based on several SAP base components. The most important components are:

- The SAP Web Application Server, which for example is used for the CRM server implementation.
- The SAP J2EE Engine, which is used to Java-based CRM components such as the Internet Sales Web application.
- The SAP Enterprise Portal, which is used to run the components in the context of People-Centric CRM.
- The SAP BW components that are used for generating BW reports.

Each of the components has its own configuration possibilities, which must be setup correctly to provide an appropriate overall level of security. The tasks to perform do not only include configuration during normal operation but also activities to be performed before, during, and after installation, such as providing secure password during installation, changing default passwords after installation, or performing customization steps (e. g. IMG activities).

Note, that it is not sufficient to setup and configure only those functions of the base component used for mySAP CRM. All available base component functions need to be configured correctly or disabled if not needed. We therefore strongly advice you to read the appropriate configuration guides available (see section "Before you Start" for references to additional information sources) for each of the components.

In addition, there are several external components on network level such as routers and firewalls that have great influence on the overall security of a mySAP CRM system landscape.

In the following sections, we will shortly describe the security dependencies between these important components and mySAP CRM. Based on examples we will further motivate why the security of the underlying components is essential for the secure operation of mySAP CRM.
SAP Web Application Server Security

The SAP Web Application Server is the technical base for many mySAP CRM components and therefore plays an important role for the mySAP CRM security. Since the mySAP CRM components are running on top the SAP Web Application Server and are also using its base functionality to implement mySAP CRM functions any configuration weakness will directly impact mySAP CRM.

The SAP Web Application Server integrates the ABAP Stack and the JAVA Stack (see also section SAP J2EE Engine Security below). Therefore both stacks need proper configuration.

A central part of mySAP CRM is the CRM server, which is running in the ABAP Stack of a SAP Web Application Server. If the standard functions and interfaces of the ABAP Stack are not appropriately configured secure operation of the CRM server component cannot be ensured.

Consider the following example:

The Web Application Server running the mySAP CRM server is also accessed by users directly with the SAPGui client. The authorization object S_TABU_DIS is available to some users to allow direct table access for another application, which must be configured this way. Unfortunately the authorization is configured with wildcards "*". This also allows these users access to the Input- and Output-Queues used in mobile client scenarios, which compromises the data by all mobile client users.

As part of its basic functions the SAP Web Application Server also offers several interfaces to the network. This also includes RFC enabled function modules or the services offered using the ICF.

Consider the following example:

A standard functionality available from the ICF is the SOAP-based RFC interface allowing RFC requests over HTTP. This interface is activated to be used by another application. The mySAP CRM scenario assumes that users only access the preceding Internet Sales Web Application. If the CRM server is not shielded properly by the firewall from http access any user is able to call any RFC functional module over http.

These two examples show that the technical basis of mySAP CRM needs proper configuration. You will find more information at the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for the SAP NetWeaver Products → SAP Web Application Server Security Guide.

SAP J2EE Engine Security

The SAP J2EE Engine is on the one hand used to implement the SAP Web Application Server Java Stack and on the other hand is available as stand-alone component. In any case it is used to run Java-based mySAP CRM components directly or SAP Enterprise Portal based mySAP CRM components indirectly by executing the SAP Enterprise Portal. The SAP J2EE Engine is a complete application server compliant to the J2EE specification. As such it offers an own user management and a role-based security environment required by the J2EE specification. In addition many services are offered to the network to conform to the J2EE specification. Thus, when using the SAP J2EE Engine to run mySAP CRM components – either as Java Stack within a SAP Web Application Server or stand-alone – all these default
features must be configured securely to allow for secure operation of mySAP CRM and to prevent undesired side effects.


**SAP Enterprise Portal Security**

The SAP Enterprise Portal is used in several mySAP CRM scenarios (e.g. Channel Management) as access platform for users. From a technical point of view the SAP Enterprise Portal is running on top of the SAP J2EE engine. Thus SAP J2EE engine security also affects the security of the SAP Enterprise Portal. The portal itself offers an own user management based on users, groups, and (portal) roles. In addition, flexible access control is provided by the different portal components. To allow for mySAP CRM integration business packages that provide appropriate iViews and role definitions must be installed into the portal.

From a security point of view, there are several areas that are important to be configured correctly: access control for the portal content, access control to the portal components, access control for the Knowledge Management (especially for repositories), and the user management configuration.

mySAP CRM is also using portal components such as News iView or Knowledge Management (KM) repositories to provide users with information or to store data. Therefore any portal misconfiguration will directly affect the mySAP CRM security.

Consider the following example:

The SAP Enterprise Portal used for the mySAP CRM scenario Channel Management is also used for Customer Self Services (CSS) in your company. Therefore many users have access to the portal. A mySAP CRM user is storing important information (e.g. conditions or notes to be kept secret) using the data store which is based on KM repositories. Unfortunately the access control settings of the KM repositories are configured to allow read access to all portal users, since the administrator wanted to provide a public available data store for the portal users, not remembering that the portal is also used for mySAP CRM. By this way any user has access to confidential CRM data.

Appropriate care during the portal configuration is also necessary because another important fact: Since mySAP CRM users are using the portal as primary access point, authentication is performed by the portal installation. To allow transparent access to the mySAP CRM server without the need to authenticate again, Single Sign-On must be configured between the SAP Enterprise portal and the mySAP CRM server. Therefore any portal user may in principle access the mySAP CRM server. This if the mySAP CRM server is mis-configured for any reason, this may allow unwanted access to functions or data.

To prevent such situations the information in this security guide and the information about SAP Enterprise Portal security will help you to configure these components appropriately. For more information about SAP Enterprise Portal security refer to the SAP Enterprise Portal security guides at the Quick Link securityguide on the SAP Service Marketplace. For general information about the SAP Enterprise Portal refer to the information found at the Quick Link nw-ep on the SAP Service Marketplace.

**Firewalls and Perimeter Security**

mySAP CRM components are distributed over several computers and need to exchange data to provide their functionality. This requires connection to a communication network. Without further restrictions network communication is in principle possible between all components connected to the network. Since there is data and functionality that requires different level of protection and must not be available to everybody in the network. Therefore firewalls – this
are network components that can filter data packets send over the network according to a set of filter rules – are used to restrict communication possibilities. Since a company network must not be accessed by external users firewalls and other access restricting components (e. g. Dial-in routers with strong authentication mechanisms) are used to protect any access path crossing the boarder – the so-called "perimeter" – between the external network to the internal company network.

Although firewall and perimeter security seems to be a general topic it directly relates to the security of any CRM installation.

Consider the following example:

A CRM system is using a database to store its data. For accessing the database the CRM software is using a technical user account, which is configured to be the standard super administrator account with a default well known password. There is no firewall used to limit possible communication possibilities to the CRM installation. In this case any user with network access any little technical knowledge is able to bypass the user authentication needed to access the CRM software by directly connecting to the database using the well known authentication information. By this way all CRM data can be accessed in any way. Now consider such a system to be accessible from the Internet (e. g. because of mobile users) without limitations for any reason.

This short example shows the importance of correctly protecting CRM systems on network communication level. The security of CRM data is therefore also influenced by the network architecture and system landscape layout used for any CRM installation.

For more information about mySAP CRM specific network security topics see auf section Network Security below. You will find more general information about network security in the context of SAP components on the SAP Service Marketplace under service.sap.com/network and service.sap.com/securityguides.

### Security of mySAP CRM Use Scenario Examples

In the following sections we will provide you with several typical use scenarios for an exemplary mySAP CRM key capability and will shortly demonstrate specific security issues that can arise for this combination.

From a security point of view any use scenario always requires a sound assessment of the protection requirements. Following that, a security policy must be defined and appropriate safeguards must be implemented. Nevertheless there are some typical threats for IT systems that depend on specific properties of the use scenario and influence the importance of single typical safeguards to be implemented.

The following examples will be structured based on the user types that typically access the CRM system. In particular:

- **Internal users**, which are own employees of your company with a strong contractual relationship.
- **Mobile** (internal) users, which induce specific technologies and risks because of the mobile nature of the access.
- **External users**, which can range from users having a partnership contract, representing users with a close relationship to your company, to Web-Shop users that buy goods or services online, representing users with a loose relationship to your company.
- **Anonymous users**, which unknown and therefore must be considered to be untrusted from a security point of view.
Note, that the different user types are normally associated with different levels of trust. The level of protection needed in your CRM scenario must nevertheless be evaluated by a threat analysis and the remaining risk your company is prepared to take according to your risk management requirements.

**Internal Users**

The mySAP CRM key capability CRM Enterprise Services is a typical Intranet use scenario. The mySAP CRM system components are located in a local Intranet subnet and client access is only performed by company employees. The following picture shows a typical system landscape setup for this scenario:

There are two Intranet network segments that are separated by a firewall or packet-filtering router: the segment containing the client machines of users and the segment, where the machines with the server-side components are located. In this typical scenario only internal users (i.e. company employees) will access the mySAP CRM system components using for example the Web browser installed on their client machines.

In this use scenario the following typical security topics play an important role:

- The firewall should shield the Backend network from all unwanted traffic (e.g. from direct SAPGui Access to the CRM Server or from direct database access with SQL-Client software). Therefore correct configuration is necessary. This also implies to know the communication ports used by the different technical components.

- Correct access control settings to functions and data. The main question to answer is: “Who is allowed to do what?”

- How can data export be made more difficult or prevented? This also means to assess the hardware situation (e.g. exist USB-Ports at client machines) and existing communication links (e.g. existing RFC-destinations or database links)

For this scenario other security topics are not relevant or do not play a dominant role, such as:

- Theft of client machines.
• Threads from anonymous attackers from the Internet.

These few examples should motivate that protection from internal attacks or just from erroneous operation by inexperienced users is the prominent security task for this use scenario. In any case, since mainly company employees with contracts are to be concerned additional legal actions can be taken in case of security violations.

Mobile Users

The mySAP CRM key capability CRM Field Sales typically involves a special type of users: mobile users. Because of the mobility special technical equipment and communication technologies must be used. In addition mobile users need to operate off-line from the server systems and therefore the necessary data must be stored locally in the mobile device, which usually is a laptop. The following picture show a typical system landscape enabling mobile access to a mySAP CRM system:

Beside other components involved MySAP CRM is using the so-called Communication Station as communication hub for mobile clients. The connection can be realized with different communication technologies. The mobility and technologies used in this scenario result in specific security related issues. Here the following topics or threats play an important role:

• User authentication is performed externally at the client machine and no backend server is involved. Therefore the security of the client machine must be ensured.

• Communication security of the communication links between mobile client and the Communication Station. Since the CRM data is synchronized using this communication link any possibility to eavesdrop the communication will compromise the data transferred. This is especially important if untrusted networks are used.

• As the mobile clients connect from external locations to the company network for synchronizing data with the CRM server, the access path must provide appropriate security for both the client itself and the company network, to protect other resources in case the client machine has been compromised. Therefore the communication station...
should be located in a secured and dedicated network and the communication relationships should be restricted by appropriate firewalls or filtering routers.

- Protection of the CRM off-line data stored at the mobile client. This is important if the mobile client is lost or gets stolen.

- General protection of the mobile client computer against viruses, worms, or other malware. This is necessary to prevent that malware is able to access the local CRM data or even the communication station during synchronization.

- Since the mobile client machine may also be used in foreign networks (e.g. customer network, Internet) or may also be used for other purpose than running the mySAP CRM mobile client, hardening should be best practice. This includes installing updates and patches, as well as reducing the software and services installed.

In addition to these prominent issues, correct access control configuration at any level (i.e. network, firewalls, machines, mySAP CRM components) must be ensured. Because of the use scenario the additional components required add more complexity to the task of configuring and operating the system secure. The appropriate sections in this guide that assist you in this task should therefore be read carefully.

**Anonymous Users**

Users that access your CRM system without prior authentication are part of almost any use scenario: Any public information for customers such as News or FAQ may be accessed this way. This may also be the case for customer forums that a company provides to allow discussions between all customers or between the customer and the company (e.g. Developer Network). The information store could be realized by using the SAP Enterprise Portal KM (Knowledge Management) Repositories. In this scenario proper access control settings for the KM repositories and the data stored within is essential. Especially if public and non-public information is stored together: Flaws in the access control setting may otherwise allow anonymous users access to non-public information intended for dedicated customers only.

We recommend treating normal users not different from anonymous users. In particular, normal users should not be trustworthier than anonymous users from a security point of view. At the end it does not matter if a normal or anonymous user compromises your data if your access control settings are not correct. Therefore sound access control and configuration settings is a precondition for secure CRM systems.
User Management and Authentication

Use

mySAP CRM uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server ABAP and Java Technology. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology and SAP Web AS Security Guide for Java Technology also apply to mySAP CRM. In addition, user administration and authentication mechanisms of the SAP Enterprise Portal are relevant for scenarios involving SAP Enterprise Portal installations such as Channel Management. Therefore, the related security recommendations and guidelines as described in the SAP Enterprise Portal Security Guide additionally apply.

In summary mySAP CRM is using the following authentication mechanisms:

- Standard SAP NetWeaver platform authentication against the ABAP stack for users directly accessing the mySAP CRM components based on ABAP.
- Standard SAP NetWeaver platform authentication against the Java stack (SAP J2EE engine) for users directly accessing the mySAP CRM components based on Java.
- Standard SAP NetWeaver platform authentication against the SAP Enterprise Portal for users directly accessing the mySAP CRM using a portal.
- Standard Windows authentication and mySAP CRM Mobile Client authentication for mobile users.

Please note, that – except for the mobile user scenarios – after the first authentication has taken place, the standard SAP NetWeaver platform Single Sign-On mechanism is used to transparently authenticate users to other components they access directly. This particularly applies to scenarios involving a SAP Enterprise Portal.

In addition to the general guidelines noted above, we include information about user administration and authentication that specifically applies to mySAP CRM in the following topics, such as customization activities for mobile client replication or for the Access Control Engine (ACE), which also involve tasks that relate to user administration and authentication. The relevant sections are:

- User Management [Seite 25]
  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with mySAP CRM.

- User Data Synchronization [Seite 46]
  mySAP CRM shares user data between different systems (depending on use scenarios). This topic describes how the user data is synchronized or which user data information must be managed in which systems.

- Integration into Single Sign-On Environments [Seite 35]
  This topic describes how mySAP CRM supports Single Sign-On mechanisms.

All this information should support you in the task of user management and authentication, which are basic pillars for your mySAP CRM system security.

Please note, that the individual subsections dedicated to the mySAP CRM key capabilities (see subsections under CRM Component Specific Security...
Guidelines in this guide) will also contain relevant information if special considerations have to be taken into account when using it.
**User Management**

**Use**

User management for mySAP CRM in general uses the mechanisms provided by the SAP Web Application Server ABAP and Java, for example, tools, user types, and password policies. In scenarios where other components are involved (e.g. a portal or mobile clients) additional user management mechanisms and tools must also be used. For an overview of how these mechanisms apply for mySAP CRM, see the sections following. In addition, we provide a list of the standard users required for operating mySAP CRM.

**User Management Tools**

The table below shows the tools to use for user management and user administration with mySAP CRM. If special considerations should be taken into account, additional information is available from the sections dedicated to the individual mySAP CRM key capabilities.

Although profile and role management is mainly a task related to authorization management, we also include this into the following table, since it also involves user accounts.

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Relevant mySAP CRM Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Web AS ABAP: Transactions SU01 (user management) and PFCG (role/profile management)</td>
<td>For any regular mySAP CRM user a user master record must be available. This user account is needed to perform access control based on profiles and roles. For more information, see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 04 → English → SAP Library → SAP NetWeaver → Security → Identity Management → Users and Roles (BC-SEC-USR). Please note, that additional actions must be performed in the ACE before a SU01 user is deleted. For more information, see section Channel Management [Seite 189] and</td>
<td>All mySAP CRM scenarios.</td>
</tr>
</tbody>
</table>
section **CRM Access Control Engine [Seite 238]**
Beside normal user management, also technical users must be created and maintained in the ABAP Stack for some mySAP CRM components. For more information, see section **SAP Internet Pricing and Configurator [Seite 151]**

<table>
<thead>
<tr>
<th>Internet User maintenance with SAP Web AS ABAP: Transaction SU05</th>
<th>For users that do not need a full user master record but must be authenticated</th>
<th>E-Commerce: SAP Internet Sales for R/3 and SAP Internet Sales for CRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>For more information, see the SAP Help Portal under help.sap.com: Documentation → SAP NetWeaver → SAP NetWeaver 04 → English → SAP Library → SAP NetWeaver → Security → Identity Management → Users and Roles (BC-SEC-USR), Section Special Functions of User and Role Maintenance – Create and Maintain Internet Users.</td>
<td>We recommend not using Internet Users created with Transaction SU05 any more. Instead Transaction SU01 should be used. For more information, see: Business Server Pages, Section &quot;Using an Internet User for BSP Applications&quot; [Extern]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Partner maintenance with SAP Web AS ABAP: Transaction BP</th>
<th>For more information, see <strong>SAP E-Commerce [Seite 107]</strong></th>
<th>E-Commerce – Internet Sales for CRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to administration pages, which are part of several mySAP CRM applications, is controlled using SAP J2EE Engine security. Appropriate SAP J2EE Engine users must be created and maintained. In some cases the Administrator of the SAP J2EE Engine must be used</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User and group management with SAP Web AS Java: Using the Visual Administrator and the security service</th>
<th>E-Commerce – E-Service – Internet Customer Self Service</th>
<th>E-Commerce – Internet Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Commerce powered by SAP NetWeaver - SAP Internet Pricing and Configurator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Guide for mySAP CRM 670 26
<table>
<thead>
<tr>
<th>Web-Based User Management</th>
<th>Used for B2B users only. For more information, see SAP E-Commerce [Seite 107].</th>
<th>E-Commerce – Internet Sales for CRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Enterprise Portal: Portal user and role administration components</td>
<td>When using mySAP CRM with a portal, each user must authenticate to the portal. To allow this a user account must be available. Depending on the SAP Enterprise Portal version the portal user administrator must create portal user accounts, since users are stored in a local database or in LDAP (EP 5.0). For EP 6.0 they can be synchronized with the mySAP CRM server, since the User Management Engine (UME) supports SAP systems as user store. During normal mySAP CRM usage the portal account is used to assign portal roles to it and to perform access control to portal components. For more information, see sections: Enterprise Sales [Seite 58] Interaction Center [Seite 156] Channel Management [Seite 156]</td>
<td>Enterprise Sales - Sales Planning and Forecasting Interaction Center - Interaction Center WebClient (when used in portal) Interaction Center - Interaction Center Manager (when used in portal) Channel Management - Channel Sales Management for High Tech Channel Management - Contracts and Chargeback for Pharmaceutical CRM powered by SAP NetWeaver - CRM Billing</td>
</tr>
</tbody>
</table>
User and User Group maintenance with SAP Web AS ABAP by CRM Customizing with Transaction SPRO (IMG activity) Access Control Engine (ACE) Administration Tool

The ACE is used to perform access control within mySAP CRM scenarios. The permissions are granted base on user groups. The group management involves assigning SU01 users to ACE user groups.

Please note, that additional actions must be performed in the ACE before a SU01 user is deleted.

For more information, see section [Channel Management][205] and section [CRM Access Control Engine][238].

Mobile Client administration console on the CRM Server

For each mobile user a user account must be created. This account is used to logon to the Mobile Client application at the mobile machine (e. g. a Laptop).

For more information see section [Field Applications][83].

MI Web Console

Used to maintain technical users for communication with PDA devices.

For more information see section [Field Applications][83].

LDAP administration application

If Internet Sales is used together with the SAP Enterprise Portal 5.0 users are stored in the Portal LDAP directory.

If an existing LDAP is used, portal user management must be performed with the administration application of the LDAP product.

For more information see section [SAP E-Commerce][107].

SQL Database administration client

The database used to store mySAP CRM data on the mobile client machine is accessed using a technical

For more information see section [SAP E-Commerce][107].
account.  

The default password of the technical account must be changed after installation.  

For more information see section Mobile Sales [Seite 84].

<table>
<thead>
<tr>
<th>Windows user management</th>
<th>mySAP CRM Field Applications: Mobile Sales and Mobile Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each person using a mySAP CRM Mobile Client a Windows user account must be generated. This account is used to logon to the Windows operating system. Depending on the Windows setup (Stand-alone vs. 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 section Mobile Sales [Seite 84] and Mobile Client Synchronization [Seite 95].</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multisite Workforce Deployment - Web Administration Tool</th>
<th>mySAP CRM Interaction Center: Workforce Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used to configure and maintain Calculation Server - JMS and SAP R/3 users. For more information, see section Interaction Center [Seite 156].</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interaction Center Agent Scheduling - Web Administration Tool</th>
<th>mySAP CRM Interaction Center: Workforce Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used to configure and maintain Calculation Server - JMS and SAP R/3 users. For more information, see section Interaction Center [Seite 156].</td>
<td></td>
</tr>
</tbody>
</table>

### User Types

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

The user types that are required for mySAP CRM include all SAP user types. The following list provides a quick overview on the user types followed by table where the different user types are given for the individual mySAP CRM key capabilities.

- Individual users:
  - SU01 Dialog users are representing the normal mySAP CRM users that are accessing the mySAP CRM functionality. Different access path are possible
requiring other user types for authentication. At the end all such users are mapped (e. g. using Single Sign-On) to the SU01 user.

- Internet users may be used for specific scenarios. In general the same policies apply as for dialog users, but used for Internet connections.
- Portal users are needed for scenarios involving a portal for accessing mySAP CRM functions.
- J2EE Engine users are used also. Theses users are mainly needed for authentication purposed when accessing administrative pages of certain mySAP CRM components running in the SAP J2EE Engine.
- Application level users are used for authentication at mySAP Mobile Clients. These users must be created using the administration console at the mySAP CRM server.

- Technical users:
  - Service users are used for running services.
  - Communication users are used for authentication of communication connections, to provide access restrictions and to enable to limit authorizations for access requests using this communication connection.
  - Background users are used for background processing, such as executing Workflow processes.


The following provides an overview on the users types used in the different mySAP CRM key capabilities.

**Enterprise Sales and Enterprise Service and Analytics**

The user type used is individual user, such as: Dialog user and Background user. Both are standard SU01 users.

Customer must create:

- Individual users to be able to use the delivered standard processes
- Initial identification parameters such as passwords and certificates for these users, since this is not provided by SAP

This is not performed by SAP

**Enterprise Marketing - Product Proposals**

If product proposals are used in Internet Sales, besides SU01 users Internet users are also required.

Product association rules for cross-, up-, and down-selling and products for top N lists can be determined in a business information system and uploaded to the CRM system. This action requires an RFC connection with a user and password.

**Enterprise Marketing - External List Management**

The application uses the following types of users:

- Dialog user
Creates and maintains Address Lists that includes activities, such as

- Creating an Address List
- Marking Process Steps that must be executed in the workflow
- Deleting an Address List

- Workflow user
  Executes the marked Process Steps in External List Management in the background through a workflow.

Both are standard SU01 users.

Field Applications - Mobile Sales and Field Applications - Mobile Service

These applications involve application level users. The customer must create these users 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 customer’s site creates individual interactive users.

Field Applications - Mobile Client Synchronization

The 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
- R/3 user to connect the Communication station to the CRM server

There is one technical user for each destination on the Communication Station.

For more information please refer to section Mobile Client Synchronization [Seite 95].

Field Applications - Mobile Sales and Service for Handheld Using CRM 4.0

In the Mobile Infrastructure Web Console, customers must maintain the following types of users:

- Administrator User
  Creates the Sync user and associates it with the application
- Sync User (device user)
  Uses the Mobile Sales and Service application on the PDA

For more information please refer to section Mobile Sales and Service for Handheld Using CRM 4.0 [Seite 104].

E-Commerce - E-Service

The following user types are used:

- SU01 user for establishing the stateless connection between CRM and ICSS.
- SAP J2EE Engine Admin for access to administrative pages.
- Portal user. The authentication value must be the SU01 User ID.

For more information please refer to section E-Service [Seite 134].

E-Commerce - SAP Internet Sales

User types are depending on use scenario, in summary the following types are used:

- SU01 dialog users and service users
- SU05 internet users (use not preferred)
- J2EE Engine users
- J2EE Engine Administrator user
- Portal users

For more information please refer to section SAP E-Commerce [Seite 107].

**E-Commerce - Selling Via eBay**

This scenario makes use of the following user types:
- SU01 dialog users and service users
- J2EE Engine Administrator user

For more information please refer to section Selling Via eBay [Seite 144].

**Interaction Center - Interaction Center WinClient**

This scenario makes use of the following user types: SU01 dialog users and service users and SU01 communication users

For more information please refer to section Interaction Center WinClient [Seite 157].

**Interaction Center - Interaction Center WebClient**

This scenario makes use of the following user types:
- SU01 dialog users
- service users
- SU01 communication users

These users are needed as follows:
- System user
  - RFC user to connect to back-end R/3 system (Optional but recommended)
    - 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.
  - JCo user to communicate between J2EE Engine and ABAP (Java configuration only)
- Individual users
  - Users on CRM Server who can access all functionalities in IC WebClient scenarios

For more information please refer to section Interaction Center WebClient [Seite 163].

**Interaction Center - E-Mail Response Management System**

Only SU01 users are used for this application.

For more information please refer to section E-Mail Response Management System [Seite 173].

**Interaction Center - Interaction Center Manager**

This application is based on:
- SU01 users and
- Portal users with appropriate role association.
For more information please refer to section Interaction Center Manager [Seite 179].

**Interaction Center - Workforce Management Services**

The workforce management services use the following user types:

- SU01 users
- J2EE Engine users
- Portal users

For more information please refer to section Interaction Center: Workforce Management Services [Seite 184].

**Channel Management - Channel Sales Management for High Tech and Channel Management - Contracts and Chargeback for Pharmaceutical**

The following user types are involved:

- SU01 users
- Portal users with appropriate role association

For more information please refer to section Channel Sales Management for High Tech [Seite 193] and Contracts and Chargeback for Pharmaceutical [Seite 198] respectively.

**Standard Users**

The different mySAP key capabilities make use of different standard users. Please refer to the individual subsections located under section CRM Component Specific Security Guidelines [Seite 54] for more information about the standard users used.
User Data Synchronization

Use

User data synchronization (i.e., synchronization of user accounts and the associated information like passwords) is generally based on the standard SAP user management synchronization mechanisms. Therefore the standard recommendations from the SAP Web Application Server apply to mySAP CRM also. You find the security-relevant information in the SAP Help Portal under help.sap.com → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for the SAP NetWeaver Products → SAP Web Application Server Security Guide.

Please note, that if multiple CRM servers are involved or if in general a central user management should be used the Central User Administration (CUA) will be involved.

With respect to and in addition to the standard SAP user management, the following has to be taken into account for mySAP CRM:

- For scenarios involving a SAP NetWeaver Portal (see SAP Help Portal under help.sap.com → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for the SAP NetWeaver Products → Portal Security Guide) for which Single Sign-On is configured with the mySAP CRM server, the portal user account name must match the mySAP CRM server user account for the same person.

- Depending on the SAP NetWeaver Portal version user accounts must be manually created or synchronized with the Portal LDAP for version 5.0 of the portal. If version 6.0 of the portal is used, the User Management Engine (UME) can be configured to make use of the mySAP CRM server as user store, then no synchronization is needed.

- For all Field Applications user accounts to be used at the mobile clients for authentication at the mySAP CRM Mobile Client application must be available. This requires manual application level actions for creating and distributing the user account information (in particular user name and the password).

More detailed information about synchronization of portal users can be found in section Internet Sales.

More information about user data distribution in Field Applications can be found in section Field Applications [Seite 83], especially subsections Mobile Sales [Seite 84] and Mobile Client Synchronization [Seite 95].
Integration with the Single Sign-On Environment

Use
Most mySAP CRM components are based on standard SAP components and therefore supports the Single Sign-On (SSO) mechanisms provided by the SAP Web Application Server ABAP and Java. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web Application Server Security Guide [Extern] also apply to the mySAP CRM.

Please note, that mySAP CRM scenarios involving multiple components for client access is using Single Sign-On. The relevant components (e. g. mySAP CRM server, SAP Enterprise Portal) must be configured for Single Sign-On to prevent the need to authenticate to the individual components.

For mySAP CRM Single Sign-On is available for all scenarios with the exception of Field Sales Scenarios where users are working locally and usually off-line at mobile machies. In this case the user must authenticate to Windows and following that to the mySAP CRM Mobile Client application. For PDAs authentication is depending on the individual PDA capabilities. For all other scenarios the supported mechanisms are listed below.

Secure Network Communications (SNC)
SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.
For more information, see Secure Network Communications (SNC) [Extern] in the SAP Web Application Server Security Guide.

SAP logon tickets
mySAP CRM supports the use of logon tickets for SSO when using a Web browser as the frontend client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system (e. g. the SAP Enterprise Portal for all mySAP CRM scenarios involving a portal). The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.

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

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

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

Please note, that using Client certificates does not automatically provide Single Sign-On, since this is only an alternative way of authentication. Nevertheless Single Sign-On based on SAP logon tickets can be used together with this kind of user authentication.
No Single Sign-On is available for Field Applications at the mobile clients, since authentication is performed using different mechanisms. Here Windows authentication is used for system access and for authentication on technical level during data synchronization and username password authentication for accessing the mySAP Mobile Client software.
Authorizations

Use


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

For scenarios involving a portal the access control mechanisms and portal role concept of the SAP Enterprise Portal are used. For role maintenance and for assigning access control restrictions the normal SAP Enterprise Portal management tools are used. Therefore the recommendations of the Portal Security Guide also apply to mySAP CRM. For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → Portal Security Guide.

In addition to these standard authorization mechanisms mySAP CRM is also using additional mechanisms important for authorization within mySAP CRM scenarios. In particular:

- The Access Control Engine (ACE) is used to configure access to your CRM data in the mySAP CRM server. Activation and configuration of the ACE is performed using system customizing. Please refer to section CRM Access Control Engine [Seite 238] in this document for more detailed information.

- For all scenarios involving mobile clients, which store replicated CRM data, additional mySAP CRM application level specific authorizations must be configured and maintained. Using these authorizations it is configured, which data should be replicated and synchronized with a mobile client. The Administration Console (Transaction SMOEAC) on the CRM server is used to configure this. For more information about this please refer to section Mobile Client Synchronization [Seite 95] in this document.

Please note, that all of the authorization mechanism must be configured and configured consistently to provide appropriate security. The information contained in this guide should support you in performing this configuration task.

As there is no general authorization configuration that fits all possible use scenarios, we strongly recommend designing an authorization concept tailored to your specific use scenario.

Standard Roles

The different mySAP key capabilities make use of different roles. Please refer to the individual subsections located under section CRM Component Specific Security Guidelines [Seite 54] for more information about the roles used.

In addition, for scenarios involving the SAP NetWeaver Portal there are also portal roles used by mySAP CRM.
Please note, that using matching roles for user accounts denoting the same person in the portal and the mySAP CRM server is important. For more information about portal roles and ABAP stack roles see section Roles in the ABAP Systems for Portal Users [Seite 246].

**Standard Authorization Objects**

The different mySAP key capabilities make use of different authorization objects. Please refer to the individual subsections located under section CRM Component Specific Security Guidelines [Seite 54] for more information about the roles used.
Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for mySAP CRM is based on the topology used by the SAP NetWeaver platform (see also section Technical System Landscape [Seite 15] for examples of mySAP CRM system landscapes). Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to mySAP CRM. Details that specifically apply to mySAP CRM are described in the following topics:

- **Communication Channel Security** [Seite 40]
  This topic describes the communication paths and protocols used by mySAP CRM.

- **Network Security** [Seite 42]
  This topic describes the recommended network topology for mySAP 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 mySAP CRM.

- **Communication Destinations** [Seite 44]
  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

**Communication Channel Security**

**Use**
The table below shows the general communication paths used by mySAP CRM, the protocol used for the connection, and the type of data transferred.

The dedicated subsections under [CRM Component Specific Security Guidelines](#) may more detailed information and may contain additional communication paths. Please refer to the appropriate individual sections.

### Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to SAP Enterprise Portal</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>mySAP CRM server to mySAP CRM server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to SAP R/3 server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to SAP BW server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>Mobile Client Machine to Communication Station</td>
<td>DCOM (Windows RPC)</td>
<td>Windows authentication, mobile client ID data, all application data</td>
<td>User information, system information and sensitive CRM data</td>
</tr>
<tr>
<td>Communication Station to mySAP CRM server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>User information, system information and sensitive CRM data</td>
</tr>
</tbody>
</table>

For further information on Communication Channel Security of specific CRM scenarios refer to:

- For the Windows DCOM connections different security levels can be configured, that also include encryption. For more information, see Mobile Client Synchronization [Seite 95].
- CRM Billing [Seite 205]
- Software Agent Framework [Seite 221]
- Interaction Center: Workforce Management Services [Seite 184].
- People Centric User Interface [Seite 226]
- E-Commerce [Seite 107]
- CRM Price List [Seite 258]
- Channel Sales Management for High Tech [Seite 193]
- Contracts and Chargeback for Pharmaceuticals [Seite 198]
- CRM Server [Seite 215]
Network Security

Use

Network security is an important aspect for the overall security of a mySAP CRM system landscape. Section Technical System Landscape [Seite 15] already discussed that the system landscape layout and the mySAP CRM components necessary depend on the application scenario and key capability to be used.

With respect to network security the following overall aspects must be taken into account for mySAP CRM:

- It is in general possible to operate the different components of mySAP CRM in different network segments. Nevertheless there are components that must be accessible by the users or customers directly (e.g. using HTTP or HTTPS protocol). This makes it necessary that these components must be located in the DMZ and thus have a higher attack potential. Therefore appropriate hardening and network access restrictions are necessary. Especially in scenarios where Internet access is necessary you may not want to make use of the same components for storing internal CRM information.

  For more information about system landscape layouts please refer to the section Technical System Landscape [Seite 15], the dedicated subsections under CRM Component Specific Security Guidelines [Seite 54], and the CRM Master Guide at the SAP Service Marketplace under service.sap.com/crm-inst. For more general information, see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Network and Communication Security → Using Multiple Network Zones.

- mySAP CRM is based on standard SAP NetWeaver components. Therefore the standard communication ports are used. For scenarios involving Web browser HTTP access port settings normally will be adjusted to fit your needs (e.g. using standard ports or several non-standard ports for different installations).


  For more information about the specific ports used by mySAP CRM components please refer to the dedicated subsections under CRM Component Specific Security Guidelines [Seite 54].

In addition to the SAP NetWeaver ports, the mySAP Field Applications involve mobile Clients and the corresponding infrastructure (e.g. Communication Station), which are based on Microsoft Windows using other communication ports.

  For more information about the specific ports used by mySAP CRM components in the Mobile Client scenarios please refer to the subsection Mobile Client Synchronization [Seite 95].

In general communication ports should only be accessible to the components that use the ports for communication. Here Firewalls, packet filters, or operating system functions for port filtering can help to shield communication ports from unwanted traffic.
• In general all mySAP CRM systems should be protected by a firewall that restricts the communication relationships.

In particular, we recommend making use of a firewall between mySAP CRM clients (e.g. SAPGUI, Web browser) and the server systems. This firewall must be configured to only allow client access to the communication ports at the allowed server systems. All other communication attempts must be prevented. Depending on the use scenario additional firewalls, packet filters, or even application level firewalls (e.g. http proxies with URL filter) should be considered depending on the necessary protection level of the data stored in your CRM system.


Beside these general information about network security for mySAP CRM, the different subsections on the mySAP CRM key capabilities under CRM Component Specific Security Guidelines [Seite 54] may contain more detailed information and recommendations about specific requirements with respect to network security.

Please remember, that there is no typical network layout for mySAP CRM in general, since this depends on the key capability used.

For further information on Network Security of specific CRM scenarios refer to:

• Mobile Client Synchronization [Seite 95]
• Interaction Center: Workforce Management Services [Seite 184]
• Software Agent Framework [Seite 221]
• Interaction Center WebClient [Seite 163]
• E-Commerce [Seite 107]
Communication Destinations

Use
The different mySAP key capabilities make use of different communication destinations. Please refer to the individual subsections located under section CRM Component Specific Security Guidelines [Seite 54] for more information about the communication destinations used.
Data Synchronization

Use

Synchronizing your CRM data appropriately between all mySAP CRM components is an important task that must also provide appropriate security because of the nature of typical CRM data. mySAP CRM is using the mySAP CRM Middleware for all data synchronization tasks. The CRM Middleware takes care about the technical processes involved in the task of data synchronization and allows configuring distribution restrictions. This helps you to control which information is made available at the different mySAP CRM components.

The mySAP CRM Middleware is used to distribute and synchronize your CRM data:

- Between different mySAP CRM servers.
- Between a mySAP CRM server and the mobile clients.
- Between the Information Warehouse server and the mySAP CRM server.
- Between the SAP R/3 server and the mySAP CRM server.

Important: Please note, that the mySAP CRM Middleware must be configured using customization actions (IMG).

For more detailed information about the mySAP CRM Middleware please refer to section Mobile Client Synchronization [Seite 95].

For more information see the individual subsections on the mySAP CRM key capabilities under CRM Component Specific Security Guidelines [Seite 54].
**User Data Synchronization**

**Use**

User data synchronization (i.e. synchronization of user accounts and the associated information like passwords) is generally based on the standard SAP user management synchronization mechanisms. Therefore the standard recommendations from the SAP Web Application Server apply to mySAP CRM also. You find the security-relevant information in the SAP Help Portal under help.sap.com → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for the SAP NetWeaver Products → SAP Web Application Server Security Guide.

Please note, that if multiple CRM servers are involved or if in general a central user management should be used the Central User Administration (CUA) will be involved.

With respect to and in addition to the standard SAP user management, the following has to be taken into account for mySAP CRM:

- For scenarios involving a SAP NetWeaver Portal (see SAP Help Portal under help.sap.com → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for the SAP NetWeaver Products → Portal Security Guide) for which Single Sign-On is configured with the mySAP CRM server, the portal user account name must match the mySAP CRM server user account for the same person.

- Depending on the SAP NetWeaver Portal version user accounts must be manually created or synchronized with the Portal LDAP for version 5.0 of the portal. If version 6.0 of the portal is used, the User Management Engine (UME) can be configured to make use of the mySAP CRM server as user store, then no synchronization is needed.

- For all Field Applications user accounts to be used at the mobile clients for authentication at the mySAP CRM Mobile Client application must be available. This requires manual application level actions for creating and distributing the user account information (in particular user name and the password).

More detailed information about synchronization of portal users can be found in section Internet Sales.

More information about user data distribution in Field Applications can be found in section Field Applications [Seite 83], especially subsections Mobile Sales [Seite 84] and Mobile Client Synchronization [Seite 95].
Data Storage Security

Use

mySAP CRM is storing your CRM data in different locations that you have configured by yourself (e. g. using the mySAP CRM Middleware to replicate data to mobile clients) or that result from properties of the technical components used for the realization of mySAP CRM (e. g. data put into log files or message queues at components used for communication path realization).

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver</td>
<td>Security Guide</td>
<td>Database Access Protection</td>
</tr>
<tr>
<td>SAP Web Application Server</td>
<td>Security Guide</td>
<td>Secure Store &amp; Forward Mechanisms (SSF) and Digital Signatures Security Aspects for the Database Connection</td>
</tr>
<tr>
<td>SAP Portal Platform</td>
<td>Security Guide</td>
<td></td>
</tr>
</tbody>
</table>

The following locations are involved in data storage security and have to be considered in the task of storing data securely:

- The mySAP CRM server is storing all mySAP CRM data in its database. Therefore the database must be secured appropriately. In addition, mySAP CRM is storing payment card information not in clear text form in the database.

  
  Please note, that storing payment card information in protected form requires installation of additional software (cryptolib) and must be activated.

  
  We recommend making use of the additional protection mechanisms for credit card information. For more information about database security refer at the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → Network and Transport Layer Security → Transport Layer Security on the SAP J2EE Engine.

- The SAP Enterprise Portal is also storing mySAP CRM data in its database, in scenarios where a portal is used. Therefore also the portal database must be protected.

  
  Note that the databases of the components mentioned above usually are located at a different physical machine. For more information about database security please refer to Database Security at the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Operating System and Database Platform Security Guides.
For all scenarios involving mobile clients the following is to be considered:

- Each Mobile Client is storing all CRM data in a local database. Because of the elevated risk of mobile clients (e.g. theft) protection of the mobile client is very important.

We recommend making use of hard disk encryption for mobile clients to generally protect all data including the mySAP CRM data. For more information please refer to Hard Drive Encryption [Seite 88].

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

For all scenarios involving Web browser access client (i.e. the machine running the Web browser) security also needs to be considered, since all information displayed by the client is normally stored in the Web browser's cache.

We recommend instructing users and customers to clear their browser cache after accessing mySAP CRM information. A logoff script could also perform this automatically if manual deletion is not considered appropriate.

### Important SAP Notes

Check regularly which SAP Notes are available about the security of the application.

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>597059</td>
<td>License conditions SAP - Cryptographic Library</td>
<td>The SAP cryptographic software is required in various components to encrypt or decrypt data for data storage and communication. For more information refer to the appropriate chapter of this guide.</td>
</tr>
<tr>
<td>397175</td>
<td>SAP Cryptographic Software - Export check</td>
<td></td>
</tr>
</tbody>
</table>
Security for Third-Party or Additional Applications

Use

mySAP CRM may be used together with third-part or additional applications that provide additional security features. In general the following applications must be considered in this context:

- Hard Disk Encryption Hard-/Software, which is recommended to be used for general protection of the data stored at mobile client machines. The product used will need to be distributed, installed, configured, and maintained to provide appropriate security. Therefore appropriate concepts as well as technical and organizational processes must be implemented at your company. For more information about hard disk encryption please see section Data Storage Security [Seite 47].

- For providing additional communication security by using SSL or SNC appropriate cryptographic libraries or products must be installed and configured. For more information, see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → SAP Web Application Server Security Guide → SAP Web AS for ABAP Technology → Protecting Your Productive System (Change & Transport System) → Security for the RFC Connections → Secure Network Communications.

- For protecting the communication path used by mobile or remote users (e.g. home office users) to connect to the mySAP CRM components (e.g. communication station or mySAP CRM server) VPN products may be used. Appropriate concepts as well as technical and organizational processes must be implemented at your company to operate the product used securely. Please refer to the documentation of the product for more information on setup and configuration.

Depending on the use scenario special applications may be useful. Please also refer to the individual sections under CRM Component Specific Security Guidelines [Seite 54] that may contain more information.
Dispersable Functions with Impacts on Security

Use

mySAP CRM consists of several components. Some components are necessary in specific use scenarios only (see also section Technical System Landscape [Seite 15] and CRM Master Guide at the SAP Service Marketplace under service.sap.com/crm-inst).

As a security best practice we recommend to install only needed components. This reduces the risk of attacks using such components in a state, where they are not configured or configured wrong.

Depending on the individual components, there may be functions that should be deactivated or configured securely if not used. For more information refer to the sections under CRM Component Specific Security Guidelines [Seite 54].
Other Security-relevant Information

Use

The following security-relevant information should be considered in the context of mySAP CRM:

- The People-Centric User Interface and other key capabilities make intensive use of JavaScript and require the use of cookies. Therefore appropriate client Web browser settings must allow the execution of JavaScript and the setting of cookies. This may impose a security risk if errors in the client Web browser exist. Please refer to sections People-Centric User Interface [Seite 226] or SAP E-Commerce [Seite 107] for more information.

- The Interaction Center WinClient makes use of the Microsoft ActiveX technology. Since this technology can impose a security risk appropriate configuration is recommended. Please refer to section Interaction Center WinClient [Seite 157] for more information.

- The Interaction Center WebClient is using active scripting of Java Applets, which requires appropriate Browser Settings. Please refer to section Interaction Center WebClient [Seite 163] for more information.

As a security best practice we recommend to advise users and customers to make use of the different trust zones that browsers offer (e.g. Microsoft Internet Explorer). The mySAP CRM components should be located in a trusted zone for which less restrictive security settings can be made. By this way users must not lower the security level of the "Internet Zone", which then may lead to successful attacks on the client browser by malicious Internet sites.

- Filtering of inputs from client side. Two kinds of attack could be attempted by hackers from this side:

  - Inclusion of malicious script code through input fields allows accessing the web site runtime context in the browser and hackers can use this means for example to mislead end users and obtain a password, credit card information or other sensitive information that will be submitted to a malicious server. This vulnerability is well-known in the literature as cross-site scripting.

  - Inclusion of SQL statement through input fields that could potentially be executed on the server resulting in an unwanted or unauthorized operation.

- Session hijacking is the ability for hackers to take over the application session of another user. This can lead to serious security problems since the hacker is then in position to act on behalf of the user, potentially accessing user’s personal information.

  Network topology between the client and the server side is an important aspect influencing the ability of a hacker to obtain the session id of a user since in a non-commuted network area all content transmitted between peer points can easily be monitored. Storing the user IP address in its session and validating it at each user request could be a way to mitigate this vulnerability, but the use of the Network Address Translation (NAT) protocol on the user side can reduce the efficiency of this solution. However, the use of the secure HTTP protocol (HTTPS) certainly helps to prevent this kind of attack.

- Hidden inputs should be used with precaution since they can easily be replaced by malicious users. For instance, if a shopping application stores item prices in hidden inputs and used thereafter by the application on the server to calculate the transaction cost, a hacker can easily replace the prices by lower ones. In addition, it should be kept in mind that hidden inputs are not as hidden as their name suggests and can easily be
consulted on the web page source. Consequently, they should not be used to store sensitive information.

- The use of the HTTP secure protocol (HTTPS) for authentication and browsing through further pages to which the user need to be authenticated is recommended to avoid eventual hackers to obtain user’s credentials and hijack user’s session as explain before.

- Cookies should be used with precaution, in particular when they are used to store sensitive information since they can be vulnerable to different kind of attack including cross-site scripting.

- HTTP headers (information retrieved from HTTP request header) should be used with precaution, for example HTTP Referrer header, since their content can easily be changed by scripts or proxies.

- Developer should also be aware of comments placed in web pages that could eventually help potential hackers to find application vulnerabilities since anybody can easily consult these comments in the page source code.

Depending on the individual components, there may be other security related information that should be considered or is important. Please refer to the sections under CRM Component Specific Security Guidelines [Seite 54] for more information.
Trace and Log Files

Use

Trace and log files can represent an important security weakness of applications if some basic precautions are neglected. Among others, well-designed applications should:

- Make use of the SAP Standard Logging & Tracing API and the SAP J2EE Engine mechanism. Besides the fact that the security consideration is that the SAP J2EE Engine manages the access and protection of the log and trace files, there are non-security related advantages that justify the use of it such as:
  - It simply avoid recoding the same functionality twice;
  - And it avoid potential performance problems of own implementation.

For more information, see the Solution Manager.

- Make sure that log file do not contain any sensitive information including but not limited as:
  - User logon information such as password;
  - Credit card information;
  - RFC traces of sensitive import/export parameters;

- Make sure to set the trace level to the minimum value to ensure that minimum information is logged in the log file;

- Tracing should be switched off in a production environment since its content is primarily intended to developers and support team.

However, even if on one hand trace and log files are an important security aspect for the reason that they can reveal important information to potential intruders, they can, on the other hand, also be exploited by system administrator to log important user activities. In this perspective, it is recommended to not wait for an attack before starting to create and review these activity logs since once the attack has occurred it’s too late to generate logs of what happened. Consequently, proactively generating and periodically reviewing activity logs to make sure that they contain sufficient information to determine what is occurring on the server and how to interpret them is the best way to prepare for a possible attack.

Finally, to ensure the availability of log files the day they will be required, these later should be backed up, and to minimize the chance of lost or corruption.
CRM Component Specific Security Guidelines

The following section contains all security-relevant information on technical components that differ from the standard settings described elsewhere in this document. To find your way better in the components, they in turn are assigned to the single key capabilities.
CRM Enterprise

Introduction
CRM Enterprise focuses on the requirement of corporate in-house employees. It supports your entire customer interaction cycle, starting with your first customer contact, through to business transactions, order fulfillment, customer service, and finally to analytical reporting.

This area provides you with specific security information for the following:

- Enterprise Sales
- Enterprise Marketing
  - External List Management scenario
  - Product Proposals
- Enterprise Service & Analytics
  - Customer Service
  - Reporting

Why Is Security Necessary?
CRM Enterprise consists of various applications based on the SAP Netweaver platform. The most of the scenarios implemented with SAP CRM based on the CRM Enterprise and have all information used in customer business, i.e. business partners, orders, marketing projects, service contracts and other.

The security aspects of CRM Enterprise are very important, because from this part of implemented scenario any business related information can be accessed.

Authorizations
The authorization check in CRM Enterprise Sales and CRM Enterprise Service & Analytics runs according to the following procedure:

1. Your own documents (authorization object CRM_ORD_OP)
2. Visibility in the organization model (authorization object CRM_ORD_LP)
3. Combination of several authorization objects

If the first two checks were not successful, this combination of different authorization objects is checked. All the checks must be successful before the user is authorized to process the required transaction. This means the user only receives the authorization to process if he is 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)

To see the list of used authorization objects and authorization fields, refer to the appropriate section of the Security Guide.
Data Storage Security

Data is stored in the CRM database. Listed below are the various types of data access:

- Read
- Write
- Delete
- Change
- Query

The payment card information can be encrypted and stored in encrypted format (if the SAP CryptoLib library is installed). For more information, refer to Payment Cards Encryption [ Seite 140].

CRM Enterprise uses the People-Centric User Interface as the web browser user interface. For more information about security see People-Centric User Interface [ Seite 226].

Security for Additional Applications

In PC-UI CRM the new Calendar ActiveX control is used.

The ActiveX control is packaged in a CAB file and uploaded to the MIME repository of the server. First time the calendar application is run; the active X control will be downloaded and installed automatically.

In this case there are 2 requirements from the client:

1. The user’s Internet Explorer settings should allow automatic download of ActiveX control. In this case, IE security settings need to be set to Medium.
2. The user should have the rights for making registry entries.

For more information, refer to Calendar (ActiveX) Control [ Seite 231].

Checklist

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar ActiveX control requirements for PC-UI</td>
<td>a) users Internet Explorer settings allow automatic download and run of signed ActiveX control?</td>
<td>a) Tools -&gt; Internet Options -&gt; Security tab, options “Download Signed ActiveX controls” and “Run ActiveX controls and Plug-ins”</td>
</tr>
<tr>
<td></td>
<td>b) user should have the rights for making registry entries</td>
<td>b) Microsoft Windows Authorization Tool</td>
</tr>
<tr>
<td>Credit Check</td>
<td>What destination is used for credit check?</td>
<td>IMG -&gt; Customer Relationship Management -&gt; CRM Middleware and</td>
</tr>
<tr>
<td>What logon procedure is used for this destination?</td>
<td>Related Components -&gt; Communication Setup -&gt; Middleware Parameters -&gt; Define Middleware Parameters SM59</td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Sales

Introduction
This topic details the security information for CRM Enterprise Sales. Enterprise Sales allows you to manage your entire sales processes consistently. In doing so, you can use various processes, such as:

- optimal planning of sales activities.
- quick analysis of the sales pipeline
- effective management of tasks and contacts as well as customers and contact persons
- organization and structuring of your sales territories
- consistent pursuit of opportunities
- processing of the sale – from inquiry, quotation and order through to invoice creation

Why Is Security Necessary?
Security is necessary, because CRM Enterprise Sales:

- accesses data in the CRM system, such as business partner information, and consists business data information, such as leads, opportunity, orders, credit cards and so on;
- from one central point has integration to the different systems (ERP back-end, APO), which is done automatically.

Therefore, it is very important to restrict access to this data.

User Administration and Authentication
The Enterprise Sales uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology [Extern] also apply to the Enterprise Sales application.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to the Enterprise Sales under User Management [Seite 25].

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the Enterprise Sales application.

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

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Web AS ABAP (Transactions SU01, PFCG)</td>
<td>For more information, see Users and Roles (BC-SEC-USR)</td>
<td></td>
</tr>
</tbody>
</table>
### User Types

The following users must be created for the CRM Enterprise Sales:

**User Types**

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory User who can access Sales, Presales and Billing transactions. Created by CRM system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>No</td>
<td>Mandatory User who can process background jobs. Created by CRM system administrator</td>
</tr>
<tr>
<td>ERP backend</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>No</td>
<td>Mandatory. User used for data exchange between CRM and ERP. Depending on RFC destination, user can be individual user or system RFC user. Created by R/3 system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>IPC User</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory. User for communication with IPC Server. Created by CRM system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>APO user</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Optional. User for</td>
</tr>
<tr>
<td></td>
<td>ERP user</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Authorizations

Enterprise Sales uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP also apply to the application.

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

The description of authorization procedure used in CRM Enterprise Sales, refer to the chapter Authorization in CRM Enterprise [Seite 55].

Standard Roles

In the following you will find the standard roles that are used by Enterprise Sales:

- Portal Role - Sales Representative
- Portal Role - Sales Assistant
- Portal Role - Sales Manager

You will find more information in the SAP Help Portal under help.sap.com → Documentation → mySAP Business Suite → SAP Customer Relationship Management → Roles → Business Package for SAP CRM 5.0.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by Enterprise Sales:

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_ACT</td>
<td>ACTVT</td>
<td></td>
<td>Business Object Activity</td>
</tr>
<tr>
<td>CRM_CO_PU</td>
<td>ACTVT</td>
<td></td>
<td>Business Object Purchase contract</td>
</tr>
<tr>
<td>CRM_CO_SC</td>
<td>ACTVT</td>
<td></td>
<td>Business Object Sales contract</td>
</tr>
<tr>
<td>CRM_OPP</td>
<td>ACTVT</td>
<td></td>
<td>Business Object Opportunity</td>
</tr>
<tr>
<td>CRM_LEAD</td>
<td>ACTVT</td>
<td></td>
<td>Business Object Lead</td>
</tr>
<tr>
<td>CRM_CMP</td>
<td>ACTVT</td>
<td></td>
<td>Business Object Complaint</td>
</tr>
</tbody>
</table>
### Network and Communication Security

The network topology for Enterprise Sales 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 Network and Communication Security to the CRM Enterprise [Seite 55] chapter also apply to CRM Enterprise Sales. Details that specifically apply to the application are described in the following topics:

- Communication Channel Security [Seite 40]

This topic describes the communication paths and protocols used by Enterprise Sales.

For more information, see the following sections at the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Network and Communication Security and Security Aspects for Connectivity and Interoperability.
Communication Channel Security
Given below are the various communication channels that are used between the components of CRM Enterprise Sales and other applications:

### Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to SAP Enterprise Portal</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>mySAP CRM server to SAP ERP server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>SAP ERP server to mySAP CRM server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and ERP data</td>
</tr>
<tr>
<td>mySAP CRM server to mySAP APO server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to SAP BW server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to IPC</td>
<td>RFC</td>
<td>Pricing conditions</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to third-party supplier (TTE or Vertex)</td>
<td>RFC</td>
<td>Tax data</td>
<td>System information and CRM data</td>
</tr>
</tbody>
</table>
Checklist

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Check</td>
<td>What destination is used for ATP check?</td>
<td>Customizing → Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Middleware Parameters</td>
</tr>
<tr>
<td></td>
<td>What logon procedure is used for this destination?</td>
<td>SM59</td>
</tr>
</tbody>
</table>
Enterprise Service and Analytics

Introduction
This key capability enables you to manage the service cycle efficiently and intelligently. It supports you in the following areas:

- Service Planning and Forecasting – including prediction and proactive planning of services and resources, and strategic service planning
- Customer Service and Support – including contract-, warranty-, and installed base management, efficient processing of service processes and case management
- Resource Planning and Optimization – including planning, assignment, and monitoring of tasks, and resource planning based on availability and qualifications
- Service Operations Management – supporting the smooth execution of core service processes with integrated controlling and logistics functionality
- Professional Services – supporting projects with processes such as opportunity management, project management, resource planning, and controlling

In each of these areas, Service Analytics functions support you in analyzing the success of your operations from diverse perspectives.

This topic details the security information for CRM Enterprise Service and Analytics

User Administration and Authentication

User Management

User

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Relationship Management</td>
<td>Normal user</td>
<td>No</td>
<td>Dialog user</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Information Warehouse</td>
<td>Normal user</td>
<td>No</td>
<td>Dialog user</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Management Tools

<table>
<thead>
<tr>
<th>Tools</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU01</td>
<td>Refer to the Users and Roles section of the Technical Operations Manual for mySAP Technology in the Help Portal (help.sap.com) under SAP R/3 and R/3 Enterprise.</td>
<td></td>
</tr>
</tbody>
</table>
| Portal Role – Service Representative / Service Manager | Technical name (Service Manager): com.sap.pct.crm.v02.servicemanager  
Technical name (Service Representative): com.sap.pct.crm.v02.servicerep |                                                     |
User Types
The Individual Users user type is used, such as:

- Dialog users
- Background users

The customers must create:

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

This is not performed by SAP

Authorizations
The following authorization objects and authorization fields are used:

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Authorization fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_CO_SE (Business Object Service contract)</td>
<td>ACTVT</td>
</tr>
<tr>
<td>CRM_CON_SE (Business Object Service confirmation)</td>
<td>ACTVT</td>
</tr>
<tr>
<td>CRM_ORD_LP (Visibility in organization model)</td>
<td>CHECK_LEV (scope of processed objects)</td>
</tr>
<tr>
<td></td>
<td>PR_TYPE (transaction type)</td>
</tr>
<tr>
<td></td>
<td>ACTVT</td>
</tr>
<tr>
<td>CRM_ORD_OE (allowed organizational units)</td>
<td>SALES_ORG (sales organization)</td>
</tr>
<tr>
<td></td>
<td>SERVICE_OR (service organization)</td>
</tr>
<tr>
<td></td>
<td>DIS_CHANNE (distribution channel)</td>
</tr>
<tr>
<td></td>
<td>SALES_ORG (sales office)</td>
</tr>
<tr>
<td></td>
<td>SALES_GROU (sales group)</td>
</tr>
<tr>
<td></td>
<td>ACTVT</td>
</tr>
<tr>
<td>CRM_ORD_OP (Own Documents)</td>
<td>PARTN_FCT (partner function)</td>
</tr>
<tr>
<td></td>
<td>PARTN_FCTT (partner function category)</td>
</tr>
<tr>
<td></td>
<td>ACTVT</td>
</tr>
<tr>
<td>CRM_ORD_PR (Business transaction type)</td>
<td>PR_TYPE (transaction type)</td>
</tr>
<tr>
<td></td>
<td>ACTVT</td>
</tr>
<tr>
<td>CRM_SEO (Business Object - Service Order)</td>
<td>ACTVT</td>
</tr>
</tbody>
</table>

Network and Communication Security

Communication Channel Security
The following communication channels are used:
• Remote Function Calls (RFC)
• BDoc type: BUS_TRANS_MSG
• ABAP SQL for the connection to database

Communication Destinations

Connection Destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Information Warehouse</td>
<td>No</td>
<td>RFC</td>
<td>User, password</td>
<td></td>
</tr>
</tbody>
</table>

Minimal Installation

The People-Centric UI requires a web browser. (See the corresponding security guidelines).
Enterprise Marketing

Enterprise marketing provides an array of tools and functions to perform marketing related activities, such as:

- Planning campaigns and trade promotions
- Creation of target groups
- Personalized product recommendations
- Complex market analysis

This area explains the security aspects associated with:

- External List Management
- Product Proposals
Product Proposals

Introduction
The product proposals consist of Cross-/Up-/Down-Selling, Accessories and Top N Lists. They use SAP Web Application Server and Business Information Warehouse. The people-centric UI of the product proposals uses the Enterprise Portal.

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Sales</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telesales</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Administration and Authentication

User Management

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The product proposals are using the normal user management of the SAP Web Application Server and require dialog users. If product proposals are used in Internet Sales, internet users are also required.

Product association rules for cross-, up-, and down-selling and products for top N lists can be determined in a business information system and uploaded to the Customer Relationship Management system. This action requires an RFC connection with a user and password.

User

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Relationship Management</td>
<td>Normal user</td>
<td>No</td>
<td>Dialog</td>
<td>Arbitrary</td>
<td>User for working with the system.</td>
</tr>
<tr>
<td>Business Information Warehouse</td>
<td>Normal user</td>
<td>No</td>
<td>Dialog</td>
<td>Arbitrary</td>
<td>User for working with the system.</td>
</tr>
</tbody>
</table>

Authorizations

The authorization object CRM_PAR manages the authorization requirements for the maintenance of product association rules (cross-/up-/down-selling). It manages authorization concerns related to:

- 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 for product association rules and display them. However, it is not possible for the user to create, change, delete, or
activate rules. It is recommended to maintain the settings of the authorization object according to the needed requirements.

There is no authorization object for top N lists. Therefore, it is not possible to handle authorization constraints, such as mentioned for the CRM_PAR authorization object.

Network and Communication Security

Communication Channel Security

Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front-end to application server and vice versa</td>
<td>DIAG</td>
<td>Application data (user interface interaction)</td>
<td>No</td>
</tr>
<tr>
<td>Application server to application server</td>
<td>RFC</td>
<td>• Certain Top N data</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Product association rule data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Certain product related data</td>
<td></td>
</tr>
</tbody>
</table>

Communication Destinations

Connection Destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Information Warehouse</td>
<td>No</td>
<td>RFC</td>
<td>User, password</td>
<td></td>
</tr>
</tbody>
</table>

Data Storage Security

The data is stored in database tables of the SAP Web Application Server. Based on the user, rights such as read, write, change, and delete are required. There is no need for a special data storage security handling.

Minimal Installation

The people centric UI requires a web browser. (See the corresponding security guidelines).

Checklist

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation or change of product association rules</td>
<td>User settings for the CRM_PAR authorization object</td>
<td>Check user settings</td>
</tr>
</tbody>
</table>
External List Management

Introduction
External List Management for CRM 5.0 is built on the following components

- Web Application Server 7.0
- EP 6.0
- BW 7.0

Please refer to the relevant security guides of these components for more details on individual component’s security aspects. For a complete list of the available SAP Security Guides, see the Quick Link securityguide on the SAP Service Marketplace.

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

Quick Links to Additional Information

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on the SAP Service Marketplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>service.sap.com/security</td>
</tr>
<tr>
<td>Security Guides</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td>service.sap.com/notes</td>
</tr>
<tr>
<td>Released platforms</td>
<td>service.sap.com/platforms</td>
</tr>
<tr>
<td>Network security</td>
<td>service.sap.com/network</td>
</tr>
<tr>
<td></td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>Technical infrastructure</td>
<td>service.sap.com/ti</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>service.sap.com/solutionmanager</td>
</tr>
</tbody>
</table>

User Administration and Authentication

User Management
The application uses two types of users: Dialog users and Workflow user. Dialog users can create and maintain external lists (Create an External List, Mark what Process Steps should be executed in the workflow, Delete an External List etc.) and Workflow user is used to execute the marked Process Steps in External List Management in background via a workflow.

User Types
The user types that are required for the external list management scenario include:

- Dialog users
  Dialog users are used for maintaining external lists (Create an External List, Mark what Process Steps should be executed in the workflow, Delete an External List etc.)

- System users
  Workflow user is used to execute the marked process steps in External List Management in the background via a workflow.

For more information on these user types, see User Types in the SAP Web AS ABAP Security Guide.
Standard Users
Workflow user, WF-BATCH, is delivered as part of standard (though not by the application directly, but by SAP Business Workflow), if missing, the user is created during SAP Business Workflow customizing.

Integration Into Single Sign-On Environments
The integration into Single Sign On (SSO) is managed by the framework and not by the application. For more information on Single Sign On, refer to the Web AS Security Guide and SAP Portal user guide.

Authorizations
The External list Management scenario uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP also apply to the External List Management scenario.

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

In CRM 5.0, the application “Maintain External List”, performs an authority check. The authority check is done on object “CRM_LIST_H”, which contains field “ACTVT”. Depending on the value, authorizations are provided to create, change, display and/or delete an external List. If the authority object is not maintained with any of the above mentioned activities, then the user can not launch the transaction “Maintain External List”. An information message is shown and the system closes the application.

In CRM 5.0, the application “Maintain Mapping Formats”, performs an authority check. The authority check is done on object “CRM_MAP_FM”, which contains field “ACTVT”. Depending on the value, authorizations are provided to create, change, display and/or delete a Mapping Format. If the authority object is not maintained with any of the above mentioned activities, then the user can not launch the transaction “Maintain Mapping Formats”. An information message is shown and the system closes the application.

In BW, the application, External List Management, relies on authority check on object S_TCODE for transaction ELM.

For the portal, the Campaign Manager role (SAP_PCC_CAMPAIGN_MANAGER) contains authorizations for BSP applications List Management and List Management Mapping.

Network and Communication Security
Communication Channel Security
The following communication paths are used by the external list management scenario, the protocol used for the connection, and the type of data transferred.

Communication Paths
The following communication channels are used by External List Management:

- Browser to Application Server (HTTP/HTTPS): Transfer of data between browser and application server if the application is used in Enterprise Portal. Please refer to security guide of EP 6.0 for security related aspects.
- Application Server to Application Server (RFC): Data is transferred from BW to CRM using RFC calls.
- Frontend to Application Server: The External List File is transferred from the frontend and stored in the application server.
The following technologies are used for these communications: HTTP, HTTPS, RFC, DIAG, File System.

**Network Security**

For information about the network security, see the Web Application Server configuration guide.

**Communication Destinations**

The application does not deliver any RFC destination or Server Group. Customers must create the RFC destinations and server groups (used in parallel processing while executing Process Steps).

**Data Storage Security**

The application uploads External List file from the frontend to the application server or uses the files already stored in the application server. These files contain Business Partner master data. The files are stored in logical path “MARKETING_FILES” in the application server. It is recommended that the physical path assigned to this logical path has sufficient access control mechanism.
Segment Builder

Introduction

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

The user of Segment Builder needs extensive authorizations. Please assign only the least.

According entries can be found at the Customizing under Customer Relationship Management → Marketing → Segment Builder → Define Segment Types and Define Reports for Master Group Generation.

Authorizations

Authorization Objects

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_SEGTYP</td>
<td>ACTVT, TYPE_ID</td>
<td>Segment Type</td>
</tr>
<tr>
<td>CRM_MGRREP</td>
<td>ACTVT, MGR_REPORT</td>
<td>Master Group Generation Report</td>
</tr>
</tbody>
</table>

You will find more information in the SAP Help Portal under help.sap.com → Documentation → mySAP Business Suite → SAP Customer Relationship Management → Roles → Business Package for SAP CRM 5.0.

- Segments
  All Segments can be protected with a standard SAP authorization object ‘CRM_SEGTYP’. Segment types can be defined unlimited. According to the selected segment type of the profile set all sub objects (profiles, target groups, sub profile sets) inherit this setting.

- Master Groups
  Reports are used for creating or updating master groups.
  This authorization object is used to check whether the user has the authorization to display, create, delete or change reports for master group generation.

If the user is not assigned to any role or profile he can do nothing with any segment object.

Standard Roles

The table below shows the standard roles that are used by CRM Enterprise Marketing.

Standard Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_PCC_CAMPAIGN_MANAGER</td>
<td>Campaign Manager in the Portal</td>
</tr>
<tr>
<td>SAP_PCC_MARKETING_ASSISTANT</td>
<td>CRM 5.0 Marketing Assistant</td>
</tr>
</tbody>
</table>
Useful SAP Notes:

- 742126: RSCRM - necessary Authorizations (315094 Recommendations for authorization in BW Reporting)
- 697572: Additional information on the Segment Builder applet - (CRM 4.0)
Digital Asset Management

Technical System Landscape
Digital Asset Management is part of the business package for SAP CRM 5.0.
Digital Asset Management uses the following parts of this business package:

- SAP Enterprise Portal
- SAP CRM backend system
- SAP NetWeaver
- SAP CRM Content Server
- SAP Trex

Additionally you can optionally use a graphics server like, for example the SAP Internet Graphics Server.

User Management and Authentication

User Management
Digital Asset Management requires user management actions in the SAP Enterprise Portal and in the CRM backend system. Please be aware that there is a relation between the portal user role and the backend authorization customizing. That means: the authorizations you grant in the backend system should fit the actions the user has access to by his portal user role. For details on this section refer to the Implementaion Guide under Customer Relationship Mangement → Marketing → Digital Asset Management → Security and Authorizations

Authorizations
DAM requires the customizing of at least one basic authorization role in the backend system to work. A reasonable usage of DAM requires a carefully designed set of portal user roles. For example: Access to some administrative sites of DAM should only be part of a specific administrator role because they show all data without further authorization check.

The DAM Repository is fully integrated in the KM Framework. It is possible to use the KM standard iViews like navigation or search to find digital asset versions, which are provided as documents. If a user clicks on the link to a document, the standard KM behavior will give him the content directly. To avoid direct access to digital asset versions it is possible to activate the CRM DAM Content Filter. You will find more information about that on the SAP Service Marketplace under service.sap.com/instguides → CRM 5.0 → CRM Core → Installation Guides.

DAM provides the possibility to control the access to digital assets in a very sophisticated way.

In general, DAM checks authorizations using the following list of authorization objects:

- DAM_ASSET
- DAM_ASSACC
- DAM_RELASS
- S_RFC
To use DAM the according users need authorizations from other/underlying components that are related to the following list of 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

(Only if you use some of the shipped BADI implementation examples.)

Be aware that this list might be incomplete since the underlying components could have introduced additional authorization checks since this documentation was written. You may use an authorization trace (for example in transaction ST01 to check this list).

Without any authorization customizing (regarding the authorization objects mentioned above) you will not be able to perform any actions in DAM or even see digital assets. For details on this section refer to the Implementaion Guide under Customer Relationship Mangement → Marketing → Digital Asset Management → Security and Authorizations

**Network and Communication Security**

**Communication Channel Security**

The following Communication Channels and Protocols are used between different components in the Digital Asset Management scenario:
### Channels and Technology

<table>
<thead>
<tr>
<th></th>
<th>Component A</th>
<th>Component B</th>
<th>Channel</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAP Enterprise Portal (Conversion Webservice)</td>
<td>Conversion Server (optional)</td>
<td>Server to server</td>
<td>http/HTTPS (secure)</td>
</tr>
<tr>
<td>2</td>
<td>SAP Enterprise Portal – Knowledge Management</td>
<td>Content Server</td>
<td>Server to server</td>
<td>http/HTTPS (secure)</td>
</tr>
<tr>
<td>3</td>
<td>SAP Enterprise Portal – Knowledge Management</td>
<td>TREX</td>
<td>Server to server</td>
<td>http/HTTPS (secure)</td>
</tr>
<tr>
<td>4</td>
<td>SAP Enterprise Portal – Knowledge Management</td>
<td>CRM 5.0</td>
<td>Server to server</td>
<td>RFC/SNC (secure)</td>
</tr>
<tr>
<td>5</td>
<td>SAP Enterprise Portal</td>
<td>CRM 5.0</td>
<td>Server to server</td>
<td>RFC/SNC (secure)</td>
</tr>
<tr>
<td>6</td>
<td>CRM 5.0</td>
<td>Content Server</td>
<td>Server to server</td>
<td>http/HTTPS (secure)</td>
</tr>
</tbody>
</table>
As you can see in the above table you have always the option between a non-secure/secure protocol.

**Communication Destinations**

The DAM iViews have an iView property that contains information about the backend system they communicate with, e. g. the CRM backend system or the TREX server. This iView Properties will usually contain the system landscape alias shipped with the business package for SAP CRM.

Digital Asset Management uses two RFC Destinations for the conversion service which have to customized in SM59 and named in the general settings of DAM.

You will find more information about that on the SAP Service Marketplace under service.sap.com/instguides → CRM 5.0 → CRM Core → Installation Guides.

**Data Storage Security**

The Digital Asset Management stores information in several places. For the security aspects of this refer to the following security guides:

- Content server security guide
- TREX security guide
- KM security guide

A server directories contain temporarily the uploaded or converted files.

Name of directory: see DAM general settings, entries CONV_INCOMING_DIR and CONV_OUTGOING_DIR. We recommend to use the available access restrictions by operating system, network, firewalls etc. to protect these directories from unauthorized access.

During file upload the files can be virus checked. To use this you have to install a third party virus checker that uses the Virus Scan Interface. For further information see the SAP NetWeaver Security Guide on the SAP Service Marketplace under service.sap.com/securityguide.

![We recommend to use signed URLs for Content Server access.]

**Dispersable Functions with Impacts on Security**

If you decide to use IGS with DAM 5.0 refer to the IGS security guide on SAP Service Marketplace under service.sap.com/securityguide.

The usage of a conversion web service from a third party may has an additional impact on the security of your solution. In this case you should refer to the security advisories of the vendor and keep in mind to protect the web service interface as well as the conversion file storage from unauthorized access.

| 7 | SAP Enterprise Portal (Conversion Webservice) | CRM 5.0 | Server to server | http/HTTPS (secure) |
**Trace and Log Files**

CRM application log entries are written if a file upload is stopped because of a virus. See application log: Object assignment: CRM_DAM Subobject assignment: CRM_DAM_MASS_UPL.

**Checklist**

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization customizing of backend roles</td>
<td>Is the access to the digital assets restricted in the desired way?</td>
<td>Perform searches and qualifications to test whether the desired restrictions apply or not.</td>
</tr>
<tr>
<td>Portal role customizing</td>
<td>Is the access to insecure portal iViews restricted?</td>
<td>Some portal iViews from KM or “DAM administration” do not filter the requested information by the DAM authorization objects. Therefore the access to such iViews should only be possible for administrators.</td>
</tr>
<tr>
<td>Virus checker installation</td>
<td>Does the system check files to be uploaded for viruses?</td>
<td>Try to upload the EICAR test virus.</td>
</tr>
</tbody>
</table>
**Campaign Management**

Campaign Management including Campaign Automation integrates several functionalities like key figure planning, email, surveys, multiple link-tracking etc. to support marketing modeling and execution.

They use the SAP Web Application Server and the Business Information Warehouse. Furthermore, the people-centric UI uses the Enterprise Portal.

**User Management and Authentication**

**User Management**

**User Management Tools**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Campaign Management including Campaign Automation is using the normal user management of the SAP Web Application Server and requires dialog users. If used in surveys etc., also internet users are needed.

Key figure planning involves an online update of data in the Business Warehouse system. This requires a RFC connection with a user and password. By customizing, the RFC user can be set to the actual dialogue user instead of a default RFC user, allowing for an individual authorization.

**User**

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Relationship Management</td>
<td>Normal user</td>
<td>No</td>
<td>Dialog user</td>
<td>Arbitrary</td>
<td>User for working with the system.</td>
</tr>
<tr>
<td>Business Information Warehouse</td>
<td>Normal user</td>
<td>No</td>
<td>Dialog user</td>
<td>Arbitrary</td>
<td>User for working with the system.</td>
</tr>
</tbody>
</table>

**Authorizations**

There are several authorization objects allowing for a specific authorization depending to a certain extent on the type of the marketing project, involving the person responsible as a central entity and so on. The complete list:

**Authorization Objects**

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_CPG</td>
<td>CRM Marketing: Business Object Campaign</td>
</tr>
<tr>
<td>CRM_CPGAGRCRM</td>
<td>Marketing: Campaign Authorization Group</td>
</tr>
<tr>
<td>CRM_CPGCTP</td>
<td>CRM Marketing: Campaign Type</td>
</tr>
<tr>
<td>CRM_CPGRES</td>
<td>CRM Marketing: Person Responsible for Campaign</td>
</tr>
</tbody>
</table>
Network and Communication Security

Communication Channel Security

In the following, there are no data requiring special protection, if a typical Marketing activity is executed like an email campaign which should reach potential customers without hurdles and which does not contain sensible data. Otherwise, you can add protection according to your needs.

The authentication and encryption protocols SNC (Secure Network Communication) and SSL (Secure Socket Layer) can be obtained from the SAP Marketplace and added to the SAP protocols DIAG (Dynamical Information and Action Gateway) and RFC (Remote Function Call), as denoted below, if desired.

Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server</td>
<td>SMTP</td>
<td>Mime-Formatted</td>
<td>In general not, but see above</td>
</tr>
<tr>
<td>Server to Server within SAP system</td>
<td>SAP DIAG (SNC)</td>
<td>Not special</td>
<td>In general not, but see above</td>
</tr>
<tr>
<td>Server to Server across SAP-Systems</td>
<td>RFC (SNC)</td>
<td>Not special</td>
<td>In general not, but see above</td>
</tr>
<tr>
<td>Internet</td>
<td>TCP/IP(SSL)</td>
<td>Not special</td>
<td>In general not, but see above</td>
</tr>
</tbody>
</table>
**Network Security**

Observe for multiple link tracking, surveys, email links and so on the usual security standards. Accordingly, use a firewall with a DMZ (Demilitarized Zone), a reverse proxy server and so on.

**Communication Destinations**

The communication destinations can be obtained from the communication paths above. Accordingly, there are:

<table>
<thead>
<tr>
<th>Communication Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
</tr>
<tr>
<td>Business Information Warehouse</td>
</tr>
<tr>
<td>SAP Web Application Server</td>
</tr>
</tbody>
</table>

**Data Storage Security**

Data are stored in database tables of the SAP Web Application Server. Depending on the user rights read, write, change and delete rights are required. There is no need for a special data storage security handling.

**Checklist**

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change a marketing project or some of its properties</td>
<td>User settings for the according authorization object</td>
<td>In case you are not authorized to perform the changes, they must be rejected.</td>
</tr>
<tr>
<td>Enter and save key figures for planning</td>
<td>Customizing for RFC destinations</td>
<td>In case a dialogue user has been maintained and you are not authorized to perform the changes, they must be rejected.</td>
</tr>
</tbody>
</table>

For more information about internet security see the SAP Help Portal at help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver Configuration → SAP Web Application Server → Management of the SAP Web Dispatcher → SAP Web Dispatcher as URL filter:
Field Applications

Field Applications enable you to utilize the marketing, sales, and service functionality in an offline environment for sales force representatives and service technicians who work in the field. Using Field Applications, field sales representatives and service technicians are able to access and update customer relationship data on their notebooks or PDAs (Personal Digital Assistants) while they carry out work in the field.

This area details the specific security relevant information for the following field applications:

- Mobile Sales
- Mobile Service
- Mobile Sales for Handheld
- Mobile Service for Handheld
Mobile Sales

Introduction
The security information in this topic is relevant for all mobile client applications, such as Mobile Sales and Mobile Service.

Important SAP Notes

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>686684</td>
<td>Tile authorizations are the same across the application</td>
</tr>
<tr>
<td>628401</td>
<td>Unable to login to the mobile client with Windows normal</td>
</tr>
<tr>
<td>559410</td>
<td>Login and Password Maintenance Functionality in 4.0</td>
</tr>
<tr>
<td>694071</td>
<td>Logon to application fails using Winlogon</td>
</tr>
<tr>
<td>622748</td>
<td>Workgroup Login Failure: Creation of Crypting Object</td>
</tr>
<tr>
<td>792979</td>
<td>Encrypting the user database password on the mobile client</td>
</tr>
</tbody>
</table>

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 the CRM Server using the administration console. In the standard delivery:

- Employees get a Bulk replication, using the publication Employee.
- Users get the Intelligent replication, using the publication Users (By Employee).

This means that for a connected site all employees are available. However, users are available for those employees that need to logon to a mobile client application.

During the first logon to a mobile client application, a mobile client user must change the default password init to a unique password. The replication of data from the CRM Server is triggered by a mobile client user using ConnTrans. Once the synchronization is complete, the data is imported into the user database, and all business components of the mobile client application are updated simultaneously.

User Types
Apart from a demo database, there are no other user types delivered with a mobile client application. The customer must create users 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 customer’s site creates individual interactive users. However, there is only one technical user (IDES) that is delivered with the mobile client application. These details are given in the table below:

<table>
<thead>
<tr>
<th>SystemUser</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User database</td>
<td>IDES</td>
<td>Yes</td>
<td>Technical User</td>
<td>IDES</td>
<td>This user is used to access the user database (SQL Server). The data for</td>
</tr>
<tr>
<td>(SQL Server)</td>
<td></td>
<td></td>
<td>SAP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
User Data Synchronization

The mobile client synchronization is performed using ConnTrans. Data is synchronized with the Consolidated Database (CDB) of the CRM Server. This means that the data is exchanged between the mobile client and the CRM Server. Synchronization can be triggered by a mobile client user any number of times and at any point in time.

For more information, see Mobile Client Synchronization [Seite 95].

Integration Into Single Sign-On Environments

There is no integration into Single Sign-On environments. Mobile client applications do not accept any logon tickets or X.509 digital certificates.

Authorizations

- You can define authorizations using the SAP CRM Mobile Authorization Management Tool (AMT).
  For more information, see:
  - Functional documentation on SAP Help Portal at help.sap.com, by choosing mySAP Customer Relationship Management → Data Exchange and Mobile Technology → CRM Mobile Technology → SAP CRM Mobile Authorization Management
  - Predefined roles that are shipped for an AMT user.
  For more information, see the topic Assigning a Predefined Role for an AMT User on SAP Help Portal at help.sap.com, by choosing mySAP Customer Relationship Management → Data Exchange and Mobile Technology → CRM Mobile Technology → SAP CRM Mobile Authorization Management Tool.

  Authorization is disabled with the default installation of mobile client applications.

Network and Communication Security

For more information, see Mobile Client Synchronization [Seite 95].

Data Storage Security

Data for mobile client applications is stored in the user database (SQL Server) on the mobile client. A mobile client user can create, modify, and delete all types of business objects and business data in a mobile client application. All changes are immediately updated in the user database. In addition to this, there are some temporary files that are stored on the local file system, WindowsUser\%Temp% of the mobile client.

Data Protection
Data protection on the mobile client is achieved using *Subscriptions* provided by CRM Middleware. This mechanism allows a system administrator to set subscriptions that allow only the data that is required for a specific user to be downloaded to a mobile client. This prevents a mobile client user from viewing or modifying data that is not relevant to the user profile.

You create a site of type mobile clients, A001 using the administration console. A mobile client user is then associated with this site. However, this user must only receive business partner information based on the postal area code.

To do this, you must first create a publication *Postal code area customer*, and then define a subscription for this publication. Various sites can now subscribe to this publication. Thus, a user can only work on the data that is relevant to the defined user profile.

For more information, refer to:

- SAP Help Portal at [help.sap.com](http://help.sap.com) and choose *mySAP Customer Relationship Management* → *Data Exchange and Mobile Technology* → *CRM Middleware*.
- [Hard Drive Encryption](#) [Seite 88](#)

**Minimal Installation**

- Implement the landscape that is recommended by SAP. For more information, see *Set Up of a System Landscape* under *mySAP Customer Relationship Management* → *SAP CRM Powered by SAP NetWeaver* → *Application Platform* → *CRM Mobile Technology* → *Implementation of CRM Mobile Client Applications* → *Standard Implementation* → *Preliminary Implementation Tasks*.

- All mobile client components that must be installed are described in the installation guide. These system resources are mandatory for the functioning of mobile client components.

  The main difference between a demo and a non-demo system is the database installation. Depending on the selection, either the demo or the non-demo database is installed. Since only the necessary components are installed, you do not have to remove any component from the productive system.

  For more information, see *Installation of Mobile Client Components* under *mySAP Customer Relationship Management* → *Data Exchange and Mobile Technology* → *CRM Mobile Technology* → *Implementation of CRM Mobile Client Applications* → *Standard Implementation* → *Preliminary Implementation Tasks*.

  A customer can decide if AMT is required. SAP recommends that you use this tool to restrict certain functions to certain groups of users.

  For more information, see *SAP CRM Mobile Authorization Management Tool* under *mySAP Customer Relationship Management* → *Data Exchange and Mobile Technology* → *CRM Mobile Technology*.

**Checklist**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check...</th>
<th>How to Check?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set authorizations for the user interface and business</td>
<td>If AMT is installed</td>
<td>Check MS Windows menu at Start → Programs → SAP →</td>
</tr>
<tr>
<td>Protection of mobile client data if the mobile client (laptop) is stolen</td>
<td>Mobile → AMT</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Protection of mobile client data if the mobile client (laptop) is stolen</td>
<td>If the hard drive in encrypted</td>
<td></td>
</tr>
<tr>
<td>For more information, see Hard Drive Encryption [Seite 88]</td>
<td>For more information, see Hard Drive Encryption [Seite 88]</td>
<td></td>
</tr>
</tbody>
</table>
Hard Drive Encryption

By stealing hard drives, criminals often attempt to access internal company data that can then be used to damage that company or to provide themselves with 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 them. Any person attempting unauthorized access without this password will only see indecipherable binary data.

Bear in mind the following aspects of encryption:

- 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 reencrypted when it is changed. The loss in performance depends on the solution used and the implementation scenario. If the encryption is implemented with hardware support, then performance loss is generally less than for a fully software-based solution.

- Emergency guidelines for application errors caused by the user or by hardware problems
  Remember that encryption is usually 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 CRM Mobile Client context. They have the following properties:

- Encryption is performed either at operating system level, or at a lower level.

- Encryption is performed either for individual files or for all data.

The following solutions are currently available:

- File Encryption Using Encrypting File System (EFS)

- Encryption of Virtual Hard Drives

- Hard drive encryption
  In hard drive encryption, the entire hard drive is encrypted. This is the following major advantage: No data areas are left unencrypted. You must even specify a password for the boot process, in order to decrypt and reencrypt data. Hard drive encryption is available both as a fully software-based solution, or including hardware support.
Some manufacturers provide an HDD password to protect the hard drive. However, HDD passwords are merely used to restrict access to the hard drive controller. The hard drive data itself is not encrypted.

File Encryption Using Encrypting File System (EFS)

From Windows 2000, Microsoft provides the option to encrypt individual files using software encryption. This makes it possible to encrypt the local CRM database. The advantage of Encrypting File System (EFS) is that it is available as standard from Windows 2000 onwards.

Products from other manufacturers also provide data encryption. This document only lists EFS because it is integrated with Windows.

In order to use EFS data encryption in the CRM Mobile Client scenario, you must first configure the MS SQL Server so that it runs on a dedicated user account. The CRM database files can then be encrypted for this user account.

Remember that encryption must be activated in the selected user account. To do this, an administrator can log on interactively via the SQL Server account and activate encryption for the database files.

We recommend that you combine all CRM-specific database files in a sub-directory and then flag this directory for encryption. Encryption key creation and management is performed automatically by Windows. This solution means that you do not need to run a Windows Public Key Infrastructure (PKI), although this is still possible if desired. The encryption keys are kept in a user profile and can be entered via 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. You can use the commands "runas", "cacls", and "cipher" to do this.

Because the MS SQL server is run as a service, the user right Log on as a service must also be assigned to the SQL server account. This is generally done automatically if the corresponding account is entered in service administration.

If encryption-related problems occur, then the machine can generally be operated normally. Only applications that access encrypted data will be unable to operate correctly. In the CRM scenario, for example, the CRM application would no longer function correctly, but the other computer functions could still be used (e.g. login, mail, other applications).

Remember the following points:

- In Windows 2000, a domain account must be used as the SQL server account. Otherwise, it would be possible for an attacker to reset the password via the administrator account. The attacker could then log on to the account and decrypt the database files.
- Additional rights need to be assigned to the SQL server account (precisely which rights are still unclear), 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 an attacker with administrator rights.
- To prevent somebody from logging on to the SQL server interactively after the initial encryption of the database files, the right to interactive logon should 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 via 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 via 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, in order to use a domain account.
- Data security depends on the operating system configuration (e.g. protection of selected account on which the SQL service is run, password quality, 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 has been copied onto 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. In order to do this, the correct software must be installed. The encrypted, virtual drive is usually 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 usually have to enter a password, which is then used to encrypt and decrypt the data when the virtual drive is accessed.

In the CRM Mobile Client scenario, 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 EFS file encryption is that security of the encrypted data relies exclusively on the encryption software and the quality of the selected encryption password. An attacker will then be unable to view the plain text data even if he/she succeeds in getting past the operating system’s access protection.

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 usually 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 for.

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 can also not 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 (e.g. 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 is started during the boot process before the operating system. A password (used for decrypting and reencrypting 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 will still only be able to access the encrypted data rather than 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 often also provide a pre-boot PKI that enables access to the encrypted disk (that is, access to the computers protected with the product) via users and groups. This PKI must then be installed and managed.

Compared with file encryption and virtual drive encryption, hard drive encryption provides general, all-round protection for all saved data. However, they place somewhat increased organizational and technical demands. Also, any 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 generally 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 again.

**Advantages of this Solution**

- Software solution, no additional hardware required.
- All data on the hard drive are 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, as 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 very little loss in performance.

Procedures that simply store the encryption key or user identities on separate hardware (for example: smart card, USB token) 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, then 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.

As a rule, a product-specific PKI must also be operated and managed.

**Advantages of this Solution**

- Depending on the implementation, better performance than for 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.

We recommend that you encrypt the hard disk, because any kind of encryption is better than none at all. However, you should consider which mechanism for encrypting the hard disk best meets your application areas and requirements.

Checklist
Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard disk Encryption</td>
<td>Recommendation fits to Your scenario</td>
<td>Choose type of encryption - File Encryption Using Encrypting File System (EFS), Encryption of Virtual Hard Drives, Hard drive encryption. Installation and usage of hard disk encryption</td>
</tr>
<tr>
<td>Recommendation does not fit to Your scenario</td>
<td>Nothing to do</td>
<td></td>
</tr>
</tbody>
</table>
**Mobile Service**

**Introduction**

Mobile Service is a key functional area of mySAP CRM that supports the field service force using mostly autonomous mobile devices. The security information relevant for Mobile Service is the same as for Mobile Sales. This is because the underlying technology and integration paradigm to CRM Server are the same.

For more information about the security details for the Mobile Service application, see Mobile Sales [Seite 84].
Mobile Client Synchronization

Introduction
This section explains the security aspects associated with the synchronization of data between the mobile client and the CRM server that is performed using the Communication Station.

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Station</td>
<td>Service Marketplace – Alias: instguides - Communication Station Guide</td>
<td></td>
</tr>
<tr>
<td>Mobile Client</td>
<td>Service Marketplace – Alias: instguides - Communication Station Guide</td>
<td></td>
</tr>
</tbody>
</table>

Important SAP Notes

⚠️ Check regularly which SAP Notes are available about the security of the application.

Important SAP Notes

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>519995</td>
<td>Communication Station: Minimum Minimum Authorizations</td>
<td>This note explains the minimum authorizations required to log on and work with the CRM server.</td>
</tr>
<tr>
<td>618527</td>
<td>BDoc messages rejected due to missing authorizations</td>
<td>This note explains how to proceed in the following scenarios:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The RFC user on the Communication Station does not have complete authorizations (SAP_ALL).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The incoming queue is automatically carried out by another user who does not have the required authorizations.</td>
</tr>
</tbody>
</table>

User Administration and Authentication

User Management
The 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
- R/3 user to connect the Communication station to the CRM server

**User**

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM Server</td>
<td>RFC Users for the internal logical connection SAPCRM_MW_RR_*</td>
<td>No</td>
<td>Communication</td>
<td>IMG</td>
<td>Communication Station Installation Guide</td>
</tr>
<tr>
<td>Communication Station</td>
<td>RFC User to the CRM Server</td>
<td>No</td>
<td>Communication</td>
<td>Communication Station Installation Guide</td>
<td></td>
</tr>
<tr>
<td>Mobile Client</td>
<td>RFC User to the CRM Server</td>
<td>No</td>
<td>Communication</td>
<td>Communication Station Installation Guide</td>
<td></td>
</tr>
</tbody>
</table>

**User Management Tools**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows user management</td>
<td>Tool provided by the Windows operating system</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At the customer site, the Windows NT administrator must create users for mobile clients.

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 5.0 on the Communication Station.

There is one technical user for each destination on the Communication Station. The R/3 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 R/3 Server.

**Authorizations**

The SAP CRM Mobile Transfer 5.0, which is a COM+ application, is installed along with the Communication Station installation. The default roles that are delivered along with this application are:

- **Administrator**
  
  Allows you to change the technical settings of the application. In addition, you can create new users under the role **User**.

  The customer is not required to create any new role. However, the customer can create new users by using the administrator role.

- **User**

  Allows mobile client users to access the application

In addition, you can execute certain tasks or define access to different objects related to the mobile client by using the Administration Console (Transaction SMOEAC) on the CRM server. The following table lists the roles that SAP delivers:
The authorization object is CRM_MW_RR. It is recommended to have at least two profiles:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_MWAC_ADMIN_ALL</td>
<td>Administration Console – Full authorizations</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_EMPL_CHANGE</td>
<td>Administration Console – maintenance of employees</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_EMPL_DISPLAY</td>
<td>Administration Console – display of employees</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_GROUP_CHANGE</td>
<td>Administration Console – maintenance of organizations</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_GROUP_DISPLAY</td>
<td>Administration Console – display of organizations</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_ILTP_CHANGE</td>
<td>Administration Console – maintenance of interlinkages</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_ILTP_DISPLAY</td>
<td>Administration Console – display of interlinkages</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_PUBL_CHANGE</td>
<td>Administration Console – maintenance of publications</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_PUBL_DISPLAY</td>
<td>Administration Console – display of publications</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_REPOBJ_CHANGE</td>
<td>Administration Console – maintenance of replication objects</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_REPOBJ_DISPLAY</td>
<td>Administration Console – display of replication objects</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SITE_CHANGE</td>
<td>Administration Console – maintenance of sites</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SITE_DISPLAY</td>
<td>Administration Console – display of sites</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SITE_INDIRECT</td>
<td>Authorization to start the indirect assignment of subscriptions (Transaction SMOEIND)</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SITE_EXTRACT</td>
<td>Authorization to start extracts through the Administration Console (Transaction SMOEIND)</td>
</tr>
</tbody>
</table>

Roles related to the Subscription Generator

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_MWAC_SUBAGENT_CHANGE</td>
<td>Administration Console – maintenance of subscription agent</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SUBAGENT_DISPLAY</td>
<td>Administration Console – display of subscription agent</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SUBSCR_CHANGE</td>
<td>Administration Console – maintenance of subscriptions</td>
</tr>
<tr>
<td>SAP_CRM_MWAC_SUBSCR_DISPLAY</td>
<td>Administration Console – display of subscriptions</td>
</tr>
</tbody>
</table>

R&R Queue Administration (Transaction SMOHQUEUE)

The authorization object is CRM_MW_RR. It is recommended to have at least two profiles:
Security Guide for mySAP CRM 670 98

Network and Communication Security

The system landscape of mySAP CRM with the mobile scenario (displayed in the figure below) consists of:

- One or more SAP R/3 systems that operate as backend servers. These R/3 systems are based on a SAP Web Application Server.
- A CRM Server that is based on a database in addition to the SAP Web Application Server. The CRM Server also includes the Middleware Broker.
- One or more Communication Stations that connect to the CRM Server. The Communication Station is a Windows 2000 based system with a Microsoft MTS (or COM+) infrastructure.
- The mobile clients that connect to one of the Communication Stations.
- Between the mobile clients and the Communication Station there might exist a RAS server or Microsoft Internet Information Server (IIS) based web server. However, these instances and the Communication Station and CRM Server might physically exist on the same machine.

- 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, refer to the DCOM Connections section below.
- To set up connections between the CRM Mobile Clients, Communication Stations, CRM Server, SAP R/3 systems, and SAP Business Warehouse (if required) can be a complicated process in a larger organization due to firewalls and network security policies, which require a more detailed knowledge on the necessary network connections.


Communication Security Zones

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
</table>

- Standard User
  Display only (Activity = 03)

- Power Users
  Display, delete entries, and operate queues (Activity = 03+06+16)
These connections are configured as RFC destinations on each system. To configure these RFC Connections

Both the connection types with their security settings are explained below:

**RFC Connections**

These connections are configured as RFC destinations on each system. To configure these destinations, you use the RFC destination tool (Transaction SM59) within a SAP Web Application Server. On the Communication Station, use QmtCnfg.exe to define the RFC destinations.

Between all these nodes it might be useful to set up firewalls. In many cases you will have at least one firewall separating the Communication Station and the other more critical instances, the SAP R/3 systems and the CRM Server.

**DCOM Connections**

**Specifying TCP/IP ports for DCOM**

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 easily be spoofed and hence it represents a security risk. Therefore, SAP recommends the usage 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 any 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.

  You must perform this activity only on the Communication Station and not on the clients.

  To do this, use the regedit32.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>
<thead>
<tr>
<th>Ports</th>
<th>This is a multi-line entry. You can enter a single port or a port range, for example, 3000-4000 on every line.</th>
</tr>
</thead>
</table>

---

Security Guide for mySAP CRM 670 99
### Network Security

To allow the mobile client users to use the SAP CRM Mobile Transfer 5.0, the following settings must be performed on the Communication Station as explained below:

1. Log on to the Communication Station.
2. Select **Start** → **Settings** → **Control Panel**.
3. Choose **Administrative Tools** and then choose **Component Services**.
4. Select **Console Root** → **Component Services** → **Computers** → **My Computer** → **Com+ Applications**.
5. Choose **SAP CRM Mobile Transfer 5.0** → **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.

- Authentication via local users on the mobile client is not supported.
- In case the mobile clients and the communication station are on different NT domains, then a trust relationship must be established for the above mentioned settings to be effective.

8. Reboot the Communication Station.

The communication occurs through DCOM that allows you to choose from a range of ports. For more information, refer to the firewall survival guide for the Communication Station.

You can set up the network infrastructure by using any of the following methods:

<table>
<thead>
<tr>
<th>PortsInternetAvailable</th>
<th>Value must be Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseInternetPorts</td>
<td>Value must be Y</td>
</tr>
</tbody>
</table>

For more information, refer to the Microsoft Paper Using Distributed COM with Firewalls by using the following link:

us/dndcom/html/msdn_dcomfirewall.asp

Subsequently, you must permit all incoming traffic using the configured port range and single port 135.

- 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 Communication Station. You can find the QmtCnfg.exe in the `<installation folder>\mobile\bin` directory on the client and the `<installation folder>\rfcsdk\crm` directory on the Communication Station.
**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 5.0 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 as 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 the SAP R/3 systems in a separate and isolated domain. In addition, you may want to place a firewall between the Communication Station(s) and the CRM Server and R/3 system(s) to allow at least incoming traffic via the ports 33xx and maybe 32xx for SAPGUI connections.
- Do not place firewalls between the mobile clients and their Communication Station. However, if you must provide firewalls, ensure that you switch to TCP/IP as the preferred DCOM transport protocol on all sides.
- 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**

This is possible either via VPN or direct dial up. SAP recommends the usage of 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. SAP recommends that the VPN connection is based on HTTPS connectivity instead of plain HTTP.

The direct dial up access is also possible though not recommended. The procedure for setting this up is as follows.

**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.

However, if 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 (maybe because there is a firewall between them), you can use one of the following methods:

- Create local users on the Communication Station with the same name and passwords as for the mobile clients and place these users in the roles configured for access to the Transfer Service. However, this is not a simple task to perform. Therefore, we recommend you to turn off the DCOM security or use the Internet scenario explained below.
- Turn off the DCOM authentication for the Transfer Service on the Communication Station and mobile clients. On the Communication Station, you must turn off the security for the Transfer Service package and configure the Authentication Level only for the Transfer Service component DOTNET.TransSrv to None. You must perform the same on all clients by using DComChfg.exe and then choosing Default Properties ➔ Default Distributed COM communication properties.
This switches the authentication off only for the Transfer Service. The security for all other services remains the same. The mobile clients possess a SiteID/DBID GUID key pair that is unique for a laptop and created during the activation of the laptop. This key pair is always used to authenticate the mobile clients towards the Middleware Broker. This authentication is not affected by switching off the authentication for the Transfer Service on the Communication Station.

**Communication Destinations**

The Communication Station and the CRM Server communicate through RFC calls. Therefore, you must create an RFC destination by using the QmtCfg.exe available on the Communication Station.

**Connection Destinations**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-NET4ABAP: Mobile Client User Administration</td>
<td>No</td>
<td>TCP/IP destination</td>
<td>To create a RFC user, refer to the IMG documentation under: Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Create RFC Users.</td>
<td>Refer to the IMG documentation under: Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Define RFC Destinations. Refer to the Communication Station Installation Guide in the SAP Service Marketplace, alias – instguides.</td>
</tr>
</tbody>
</table>

**Data Storage Security**

The data recorded by the sales representative 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 the CRM server through the communication station and stored in the consolidated database (CDB) on the CRM server.

During synchronization, the data is persisted 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 the 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 Communication Station.

We recommend you to set the trace level to the minimum value to ensure that minimum information is logged in the log file.
Mobile Sales and Service for Handheld Using CRM

Introduction

The mobile sales and service application for handheld is based on the following components:

- Mobile Infrastructure
- SAP Web Application Server
- mySAP CRM
- MSA/MSE

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server</td>
<td>SAP Security Guide</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td>MI 2.1 SP02</td>
<td>SAP Security Guide</td>
<td>→ SAP Mobile Engine</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

The security for the application is required to protect:

- Attacks from the Internet
- Password theft
- Data mismatch for each user

User Administration and Authentication

User Management

The user management is performed by the Mobile Infrastructure Web Console. There is no user management in the PDA device. The PDA does not have an administrative user management principle. However, a one time setting of userID->applicationID->MobileID is performed by default during the setting up of the application.

In the Mobile Infrastructure Web Console, customers must maintain the following types of users:

- Administrator User
  Creates the Sync user and associates it with the application
- Sync User (device user)
  Uses the Mobile Sales and Service application on the PDA

No standard users are delivered. Therefore, the customer must create the required users. The administrator for the customer will create the handheld (Sync user) users for the application. Subsequently, these sync users can use the handheld application to synchronize data with the CRM server.

- The sync users are authenticated by SAP authentication on the CRM system.
The method by which sync users obtain their initial identification parameters depends on the company’s policy.

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
</table>

User Data Synchronization

The synchronization of user data is explained below:

- Application synchronization
  The application is synchronized with the Mobile Infrastructure Web Console.

- Data synchronization
  The application data is synchronized with CRM.

The synchronization is managed by the Mobile Infrastructure as follows:

- Application synchronization
  The application associated with the user is downloaded to the handheld device.

- Data synchronization
  The CRM data applicable to the user is downloaded to the handheld device.

When the handheld user starts synchronization, the CRM data applicable to the user is exchanged.

Integration Into Single Sign-On Environments

The Authentication to enable integration is part of the Mobile Infrastructure.

Authorizations

No authorization object exists for the application.

Network and Communication Security

Communication Channel Security

The following Communication channels are used:

- PDA to the Mobile Infrastructure
- PDA to CRM online

This communication is managed by the Mobile Infrastructure through TCP/IP.

The following technology is used for this communication:

- HTTP
- HTTPS
- File System

The following data is transferred:
• The user relevant CRM data maintained in CRM is downloaded and
• The business data created on the handheld is uploaded.

**Network Security**
You can operate the different components, such as MI, SAP WAS, and CRM, in different network segments.

• This is possible only if the components are maintained in different network segments.
• The communication between the different components is achieved through an HTTP port.
• The firewall settings depend on the company’s policy.
• During the synchronization of data, the PDA must be connected to the network to transfer data to the CRM system.

**Communication Destinations**
The communication destinations are maintained by the Mobile Infrastructure.

**Data Storage Security**
The data is stored locally on the PDA in the SAPMobileEngine as OBJ files during the downsync from the CRM system or when different business operations are performed using the application.
The access rights, such as read, write, and change depend on the operation performed by the application.

• The access to data is protected by Mobile Infrastructure.
• The application requires the web browser as the user interface. However, the cookies are not used to store data.

**Other Security-Relevant Information**
The front end (User interface) of the application uses the JavaScript and applet. To save any information from the applet to the application, the security policy file must be updated.

This is applicable only if the CRM application is used as a desktop application. In a PDA, this is managed by the mobile engine.
SAP E-Commerce

E-Commerce scenarios consist of ABAP based functionality on the CRM Server and Java based functionality on the Java Stack of NetWeaver (J2EE Engine).

The Java based applications running on the J2EE Engine provide the user interface to the functionality located in the CRM Server. In most cases the UI is exposed to the Internet. It is therefore a potential target for various attacks. It is therefore essential for you to protect your E-Commerce applications in order to protect your business and investment.

Introduction
This section gives you the information helping you to determine and implement the level of security you would like to achieve when running SAP E-Commerce

This chapter covers the following scenarios:

- SAP E-Commerce for mySAP CRM
- SAP E-Commerce for mySAP ERP E-Commerce-related parts of Channel Management (mostly web applications)
- SAP E-Service

The abbreviation E-COMMERCE is used as synonym for all SAP E-Commerce web applications.

The security relevant topics of the dependent components, such as the J2EE Engine, are described in detail in the corresponding security guides.

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most- Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver</td>
<td>J2EE Guide</td>
<td>How to configure SSL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>How to install SNC</td>
</tr>
<tr>
<td>Channel Management</td>
<td>CRM Access Control Engine</td>
<td>[Seite 238]</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>CRM Access Control Engine</td>
<td>[Seite 238]</td>
</tr>
<tr>
<td>SAP NetWeaver Portal</td>
<td>EP</td>
<td></td>
</tr>
</tbody>
</table>

Why Is Security Necessary
Security is critical to SAP E-Commerce installations. E-Commerce enables customers to do their B2B or B2C business over the internet. Your application can be the target of many different attack scenarios. The table below provides an overview on some attack scenarios and the corresponding chapters giving you information how to protect your application:

Attack Scenarios

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Description</th>
<th>Relevant Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken Access Control</td>
<td>Restrictions on the activities that the authenticated users can perform are not properly enforced.</td>
<td>User Administration and Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Storage Security</td>
</tr>
</tbody>
</table>
## Important SAP Notes

### SAP Notes

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>828420</td>
<td>Composite Security Note: CRM E-Commerce</td>
<td>This note is the central entry point for up to date information on CRM E-Commerce. Please check this note regularly</td>
</tr>
<tr>
<td></td>
<td>NetWeaver Java Stack composite security note</td>
<td>Check this note for news related to security of the NetWeaver Java stack</td>
</tr>
</tbody>
</table>

## User Administration and Authentication

The type of the user administration differs depending on the use of SAP E-Commerce for mySAP CRM, SAP E-Commerce for mySAP ERP or SAP NetWeaver Portal as explained in the following sections.

E-Commerce runs by using SU01 and SU05 user types.

### User Management Tools

#### User Management Tools for all SAP E-Commerce Scenarios

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web AS Java user management using the Visual Administrator</td>
<td>Access to administration pages, which are part of every E-Commerce web application, is controlled using WebAS Java security.</td>
<td>Is automatically activated after deploying the web E-COMMERCE web applications</td>
</tr>
<tr>
<td>Web-based user management</td>
<td>For configuration information, see SAP Solution Manager.</td>
<td>Only applicable for B2B users with SU01 user type.</td>
</tr>
</tbody>
</table>
User Management Tools: SAP E-Commerce for mySAP ERP

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User management for the ABAP Engine (transaction SU01)</td>
<td>Refer to the SU01 Documentation.</td>
<td>Possible for B2B, B2C, Shop Management, and user management applications.</td>
</tr>
<tr>
<td>Maintenance of roles and profiles via transaction PFCG</td>
<td>Refer to the SU01 and PFCG Documentation.</td>
<td>For information on the login configurations for ERP E-Commerce, see the Solution Manager.</td>
</tr>
<tr>
<td>SU05 (Internet Users)</td>
<td>Refer to the SU05 Documentation.</td>
<td>Only possible for B2B and B2C applications.</td>
</tr>
<tr>
<td></td>
<td>We recommend you to use SU01 users if possible.</td>
<td>For information on the login configurations for ERP E-Commerce, see the Solution Manager.</td>
</tr>
<tr>
<td>User Management Engine (UME)</td>
<td>Refer to UME documentation and note 713472.</td>
<td>Only possible for B2B, shop management, and Web-Based User Management with SU01 user type.</td>
</tr>
</tbody>
</table>

User Management Tools: SAP E-Commerce for mySAP CRM

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance of roles and profiles via transaction PFCG</td>
<td>Refer to the BP Documentation Creation of business partners with the role Internetuser.</td>
<td>For more information, see the configuration information in the Solution Manager.</td>
</tr>
<tr>
<td>Business Partner Maintenance (transaction BP)</td>
<td>Refer to the SU05 Documentation.</td>
<td>Only possible for B2B and B2C.</td>
</tr>
<tr>
<td></td>
<td>We recommend you to use SU01 users.</td>
<td>For more information, see the configuration information in the Solution Manager.</td>
</tr>
<tr>
<td>SU05 (Internet Users)</td>
<td>Refer to the SU05 Documentation.</td>
<td>Only possible for B2B and B2C.</td>
</tr>
<tr>
<td></td>
<td>We recommend you to use SU01 users.</td>
<td>For more information, see the configuration information in the Solution Manager.</td>
</tr>
<tr>
<td>User Management Engine (UME)</td>
<td>Refer to the UME Documentation and note 713472.</td>
<td>Only possible for B2B and Web-Based User Management with SU01 user type.</td>
</tr>
</tbody>
</table>
### User Management Tools when using E-COMMERCE within Portal (Channel Management)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management Engine (UME)</td>
<td>Refer to the UME Documentation and note 713472.</td>
<td>Only up to EP 6.0 Usually E-COMMERCE application and EP 6.0 must be deployed on the same J2EE Engine (stand NW4). Only possible for B2B and Web-Based User Management with SU01 user type.</td>
</tr>
</tbody>
</table>

### User Types

User types for all E-Commerce Applications

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebAS Java</td>
<td>Administrator</td>
<td>Yes (part of WebAS Java installation)</td>
<td>User Administered on WebAS Java</td>
<td>As defined during installation of WebAS Java</td>
<td>This user can be used to enter the E-COMMERCE Administration pages. For more information, see Link to XCM Tutorial. It is recommended to create a new user with less rights for administration of E-COMMERCE application instead of using the WebAS Java Administrator (see next).</td>
</tr>
<tr>
<td>WebAS Java</td>
<td>isaadmin</td>
<td>No</td>
<td>User administered on WebAS Java</td>
<td>No</td>
<td>It is recommended to create this user after the Installation of the WebAS (together with the CRM Java applications). For more information, refer to the</td>
</tr>
</tbody>
</table>
### User Types for SAP E-Commerce for mySAP ERP

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERP</td>
<td>Anonymous user for stateless connection</td>
<td>No</td>
<td>SU01 service user</td>
<td>No</td>
<td>SU01 User for establishing the stateless connection between ERP and E-COMMERCE. This user must be maintained in XCM Administrator Tool. For example, this user is used for determining the ERP release before E-COMMERCE user logs in or for reading the ERP catalog or customizing.</td>
</tr>
<tr>
<td>ERP</td>
<td>E-COMMERCE user</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>The user that logs into E-COMMERCE. The full state E-COMMERCE connection is established with it and sales documents are created using this connection. Only relevant if the login type is 4, 7, 8, or 9. This corresponds to the XCM settings R3_SU01User, R3_SU01UserContactPerson, R3_SU01UserStandalone, or R3_SU01Customer_LoginEmail in component usertype. For more information, see the Solution Manager.</td>
</tr>
<tr>
<td>ERP</td>
<td>E-COMMERCE user</td>
<td>No</td>
<td>SU05</td>
<td>No</td>
<td>The user that logs into E-COMMERCE. The full state E-COMMERCE connection is established with the anonymous SU01 user. Only relevant if the login type is 0, 1, or 2. This corresponds to the XCM settings R3_SU05Customer_LoginCustomerNo, R3_SU05Customer_LoginEmail, or R3_SU05ContactPerson_LoginContactPersonId in component usertype. For more information, see the Solution Manager.</td>
</tr>
</tbody>
</table>

### User Types for CRM E-Commerce and Channel Management

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM</td>
<td>Service (anonymous) user for stateless connection</td>
<td>No</td>
<td>SU01 service user</td>
<td>No</td>
<td>SU01 User for establishing the stateless connection between</td>
</tr>
</tbody>
</table>
Security Guide for mySAP CRM 670

User Data Synchronization

In some cases it is necessary that the user data will be maintained in different systems to implement integrated scenarios. If the user data should be synchronized in different ABAP-based systems, the standard functionality of Central User Administration (CUA) should be used. For more information about this, please refer to the CUA documentation.

The synchronization of user data outside of the ABAP systems will be realized through the User Management Engine (UME). In this case the principle of double data maintenance will be used, i.e. the data will be maintained at first in an ABAP backend (CRM or R/3 system) and after that the same user data will be maintained in the UME system.

The user data for B2B-based E-Commerce applications should be maintained by the E-Commerce Web-Based User Management application. The support of CUA and UME for E-Commerce applications will be supported only by this application.

Support of EP 5.0 in E-COMMERCE for CRM

Since CRM 5.0 E-COMMERCE applications do not support EP 5.0, only up to EP 6.0 is applicable.

Support of UME (User Management Engine) and EP 6.0

The E-COMMERCE applications, B2B shop (all scenarios) and Web-Based User Management support UME and EP 6.0 concurrently as UME is included in EP6.0.

The replication of user data between E-COMMERCE and UME occurs directly through UME-API. As a result, there is no external connection that must be protected. In addition, E-COMMERCE and UME must be deployed usually on the same J2EE Engine and on the same instance. More details about this scenario can be found in the SAP Note 713472.

Regarding synchronization of user data and user roles between E-Commerce user structure and UME user structure, it exist a configuration file where this data will be maintained. For more details please see SAP Note 713472.

In addition E-COMMERCE Applications provide optionally the usage of UME logon application. In such a case, UME provides its authentication services that will be called before the logon of E-COMMERCE applications. After a successful authentication, UME creates a Single Sign-On ticket which will be transmitted to the E-COMMERCE application. For more information, refer to the UME documentation.

If the user storage of UME is connected to the same ABAP-based backend as the E-Commerce application, the replication between E-Commerce and UME mustn’t be performed. In this case it is sufficient, if the Web-Based User Management application creates only users based on SU01 User ID.
Logon Processes
Since CRM release 5.0 the most E-Commerce applications use one central logon module implementation. This logon module includes different logon procedures: UME- and E-Commerce Logon Procedure.

- The E-Commerce Logon Module corresponds to the logon functionality of the earlier releases of E-COMMERCE. In particular for upgrade scenarios this procedure should be used (e.g. to get support to login with SU01 User Alias).

- The UME Logon Procedure base on the UME Logon application which is a part of the core services of SAP J2EE Engine 6.30 (and newer). In such a case, UME provides its authentication services that will be called before the E-Commerce application will be processed. With UME Logon Service further logon methods are available for example, SAP logon tickets (SSO2) or X.509 digital certificates. For more information, refer to the UME documentation and about E-Commerce specific settings to the note 805713. It will be recommended to use UME Logon Procedure as default.

Independent from the used logon procedure, all E-Commerce applications which contain the central logon module, accept SAP logon tickets (SSO2) for logon procedure.

Integration Into Single Sign-On Environments
Independent from the used logon procedure, all E-Commerce applications which contain the central logon module, accept SAP logon tickets (SSO2) for logon procedure.

If UME support is enabled, further logon methods are available for example, X.509 digital certificates. For more information, refer to the UME documentation.

In Channel Management, the SSO ticket is issued by the portal environment, which is created when the user logs into the portal. Subsequently, this ticket is used consistently throughout the portal even for login to the E-COMMERCE environment. For more information, see E-Commerce.

Authorizations

Authorizations based on user roles
The following table lists the roles that are created on the WebAS Java for each E-COMMERCE application when the application is installed.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isaadmin</td>
<td>Automatically assigned to the administrators group after installation. All users assigned to this role can enter the E-COMMERCE Administrator area. This role is used by system administrators when configuring the web application, for example, when using Extended Configuration Management (XCM). It is recommended to create a new user for E-COMMERCE administration and to assign it to this role. This prevents E-COMMERCE web application administrators to have full access to the WebAS Java.</td>
</tr>
<tr>
<td>Ccms</td>
<td>Automatically assigned to the administrators group. This role is only used internally by the application for reporting of version/configuration information to the central monitoring system. You do not have to do any changes here.</td>
</tr>
</tbody>
</table>
The following table lists the shipped E-Commerce user roles. For each E-Commerce application, individual user roles for the Internet Users and Service Users (anonymous users) are provided. For more information on these roles and how to use these to configure own user roles, see the Solution Manager documentation.

### User Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2B_FULL</td>
<td>B2B with full document authorization</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2B_ORDER</td>
<td>B2B with full order and display sales order document authorization.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2C</td>
<td>Full B2C authorization (when the user is logged on). This role will be assigned to a reference user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_TU_B2C</td>
<td>B2C service (anonymous) user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_SHOPADMIN</td>
<td>Full shop management authorization.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_TU_SHOPADMIN</td>
<td>Shop management service (anonymous) user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_BOB_FULL</td>
<td>BOB with full sales order document and quotation authorizations.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_TU_BOB</td>
<td>BOB service (anonymous) user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_HOM_FULL</td>
<td>Hosted Order Management with full authorization.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_HOM_VIEW</td>
<td></td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_TU_HOM</td>
<td>Hosted Order Management service (anonymous) user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_USERADMIN</td>
<td>Full User admin authorization; this is the role for a super user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_SU_USERADMIN</td>
<td>User admin service (anonymous) user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_TU_AVW</td>
<td>Auctioning via web shop anonymous user. Used in logon and background tasks like determining the winners for auctions.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_AVW_WU_SELLER</td>
<td>Creates and manages auctions in Auctioning via web shop.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_AVW_WU_ADMIN</td>
<td>Configures the background tasks required for auction management process in Auctioning via Web shop.</td>
</tr>
<tr>
<td>SAP_PCC_COL_PARTNEREMPLOYEE</td>
<td>Channel Management – Partner Employee</td>
</tr>
<tr>
<td>SAP_PCC_COL_PARTNERMANAGER</td>
<td>Channel Management – Partner Manager</td>
</tr>
<tr>
<td>SAP_PCC_COL_PARTNERMANAGER_CC</td>
<td>Channel Management – Partner Manager Channel Commerce</td>
</tr>
</tbody>
</table>

### SAP E-Commerce in mySAP ERP

Refer to the configuration documentation in the Solution Manager for information on the authorization roles relevant for SAP E-Commerce in mySAP ERP.
Authorization Roles

<table>
<thead>
<tr>
<th>Authorization Role in the backend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_ISA_B2C_RFC</td>
<td>Role for the B2C RFC user</td>
</tr>
<tr>
<td>SAP_ISA_B2C_FULL</td>
<td>Role for the SU01 B2C users. This role should be assigned to the reference user, not to users directly (performance reasons)</td>
</tr>
<tr>
<td>SAP_ISA_B2B_RFC</td>
<td>Role for the B2B RFC user</td>
</tr>
<tr>
<td>SAP_ISA_B2B_VIEW</td>
<td>B2B, only view catalog and maintain templates</td>
</tr>
<tr>
<td>SAP_ISA_B2B_ORDER</td>
<td>B2B, create orders</td>
</tr>
<tr>
<td>SAP_ISA_B2B_FULL</td>
<td>Full B2B authorizations</td>
</tr>
<tr>
<td>SAP_ISA_BOB_FULL</td>
<td>Full BOB authorizations</td>
</tr>
<tr>
<td>SAP_ISA_SHOPMGMGT_RFC</td>
<td>Shop Management RFC user</td>
</tr>
<tr>
<td>SAP_ISA_SHOPMGMGT_FULL</td>
<td>Full Shop Management authorizations</td>
</tr>
<tr>
<td>SAP_ISA_UADM_RFC</td>
<td>User Management RFC user</td>
</tr>
<tr>
<td>SAP_ISA_UADM_SUPERUSER</td>
<td>User Management: customer super user. Has authorizations to maintain users for his/her company</td>
</tr>
</tbody>
</table>

Channel Management

In Channel Management, the roles are delivered along with external services objects included in the user menu. The external services for PC-UI are delivered, with the objective to provide a comprehensive list of all authorization objects used in a PC-UI application. In addition within these services, also the predefined values, if there are any, for the authorization objects, can also be defined. For applications(PC-UI) relevant to Channel Management we use this method to assign authority objects and their values to different roles. The list of external services assigned to a role can be viewed in the Menu tab of Roles, directly under the Portal role node.

Please note that these external services are defined only for PC-UI applications in the role. For applications/views, in the role, which are of different kind, the authorizations would be taken care of in the delivered roles, same like as before.

With external services, the values delivered as 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 delivered values to the customer namespace and then change or maintain these values. This is performed in transaction SU24. For details, refer to SAP Note 444686, Missing authorizations in generated profiles.

Authorizations based on the CRM Access Control Engine

The Access Control Engine (ACE) is another important step towards Authorizations in Channel Management and SAP E-Commerce. This is a new tool developed to control access for users. ACE is used in conjunction with ABAP Authorization concept to provide full security to the applications and data.

In Channel Management and E-Commerce, the data security is provided by ACE. The access to the data for the users is defined through a set of predefined rules in ACE. These set of rules are applied to the data when it is being created and stored and from this an ACL is generated. This ACL is then used during runtime to determine the extent of access the user has to the data.
Currently the ACE checks run only in CRM backend. To get the ACE up and running, the customers must go through certain steps, as defined in CRM Access Control Engine [Seite 238]. 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 the Implementation Guide under Customer Relationship Management → Basic Functions → Access Control Engine.

**Network and Communication Security**

**Communication Channel Security**

The following Communication Channels and Protocols are used between different components in an E-Commerce scenario.

**Channel and Technology**

<table>
<thead>
<tr>
<th>Component A</th>
<th>Component B</th>
<th>Channel</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browser</td>
<td>HTTP Server (Reverse Proxy)</td>
<td>Front-end to server Communication with web browser</td>
<td>HTTP/HTTPS (secure)</td>
</tr>
<tr>
<td>HTTP Server</td>
<td>J2EE Engine/E-COMMERCE web application</td>
<td>Server to server Requests from web browser are forwarded to E-COMMERCE application running on J2EE engine. Responses from E-COMMERCE are forwarded to the web browser.</td>
<td>HTTP/HTTPS (secure)</td>
</tr>
<tr>
<td>J2EE Engine/E-COMMERCE web application</td>
<td>CRM or ERP system</td>
<td>Application to server Java based E-COMMERCE application executes application logic running on the SAP system.</td>
<td>RFC/SNC (secure)</td>
</tr>
<tr>
<td>J2EE Engine/E-COMMERCE web application</td>
<td>IPC</td>
<td>Application to server Communication for product configuration/pricing</td>
<td>RFC/SNC (secure)</td>
</tr>
<tr>
<td>J2EE Engine/E-COMMERCE web application (CRM)</td>
<td>TREX</td>
<td>Application to server Communication for getting catalog data</td>
<td>RFC/SNC (secure)</td>
</tr>
<tr>
<td>J2EE Engine/E-COMMERCE web application (ERP)</td>
<td>TREX</td>
<td>Application to server Communication for getting catalog data</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>CRM or ERP</td>
<td>TREX</td>
<td>Server to Server for catalog replication</td>
<td>RFC</td>
</tr>
</tbody>
</table>
As you can see in the above table you have always the option between a non-secure or secure protocol. The next chapter gives you the information to decide which protocol fulfills your security requirements.

**Guidelines Selecting a Secure Communication Channels**

**Secure Socket Layer (SSL)**

The SSL encryption protects the data (e.g. log on data to the web shop) from potential eavesdroppers, providing a higher degree of privacy for the communications. The data is also protected from manipulation – any changes made to the data during transfer are detected.

For general information about SSL and how to set up SSL on the WebAS refer to the SAP NetWeaver Security Guide.

You have to configure the HTTP and HTTPS ports in XCM if you intend to use SSL in your E-Commerce application:

```
XCM → General Application Settings → Customer → <application name e.g. b2b> → <appname>config → http.port.core and https.port.core
```

**Communication Channel between Web Client and HTTP Proxy or WebAs Java**

It is recommended to use SSL to protect the traffic between the web browser and the HTTP server or the WebAS.

SSL is turned in the various E-Commerce applications (e.g. B2B, B2C) after installation.

- In B2C the application switches to SSL when entering the check out process.
- In B2B or other application having a log on screen at the beginning the application automatically switches to SSL when entering the logon screen.

Whether SSL is used in configured in the XCM Administration tool: General Application Settings → Customer → <web application name e.g. b2b> → SSL-enabled

**HTTP based Communication Channel between WebAs Java and TREX**

If you want to secure the HTTP based communication channel to the TREX server refer to the following documentation

- SAP Note 819143

**Secure Network Communication (SNC)**

SNC is used to secure the data communication paths between the various SAP System components.

There are three levels of security protection you can apply. They are:

- 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 E-Commerce is Privacy protection. This is the maximum level provided by SNC.

In order to set up SNC in E-Commerce you have to perform the following steps:

- Set up SNC on your WebAs Java server and the Backend system you are communicating to (e.g. CRM or ERP). You have to perform various installation steps
like installing an external security product creating an PSE, credentials etc. For further information refer to the SAP NetWeaver Security Guide.

- You have to configure SNC based connection data in every web application of your E-Commerce scenario (e.g. B2B, B2C, Shop administration etc.)

This is done in Extended Configuration Management (XCM) in using the 'jco' configuration component. Select either the 'secure server connect' or the 'secure group connect' base configuration while creating the connection configuration.

**SAP E-Commerce for mySAP CRM**
Communication Destinations

Connection Destinations from E-COMMERCE Web Applications

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to CRM/SAP system</td>
<td>No</td>
<td>RFC</td>
<td>Refer to the</td>
<td>Technical user used for stateless (anonymous) communication with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Authorizations section.</td>
<td>backend system. Configured using XCM tool after installation.</td>
</tr>
<tr>
<td>Connection to IPC server</td>
<td>No</td>
<td>RFC</td>
<td>No</td>
<td>Configured using XCM tool after installation.</td>
</tr>
<tr>
<td>Connection to TREX</td>
<td>No</td>
<td>RFC</td>
<td>No</td>
<td>The TREX can be configured using manual configuration or dynamic configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>in the XCM. When using Dynamic</td>
</tr>
</tbody>
</table>
configuration, the values of the RFC destination to the IMS server are normally retrieved automatically from the underlying backend CRM system (if the value of the parameter "useDynConnParams" is "true"). When you choose this setting, you do not have to specify any other parameter for this component. The other possibility 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 web server or different web servers are able to access different IMS servers, thereby implementing web load balancing or high availability. The distribution and update management of the indexes between such different IMS servers must be performed by other mechanisms (E-Commerce does not provide support for this).
At present, no security level is set for both the configurations. After the implementation, the RFC connection between the TREX and the CRM system will be secured using SNC. We can also use other methods, such as VPN.

### Connection Destinations

**Connection Destinations from E-COMMERCE Web Applications**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to CRM/SAP system</td>
<td>No</td>
<td>RFC</td>
<td>Refer to the Authorizations section.</td>
<td>Technical user used for stateless (anonymous) communication with the backend system. Configured using XCM tool after installation.</td>
</tr>
<tr>
<td>Connection to IPC server</td>
<td>No</td>
<td>RFC</td>
<td>No</td>
<td>Configured using XCM tool after installation.</td>
</tr>
<tr>
<td>Connection to TREX</td>
<td>No</td>
<td>RFC</td>
<td>No</td>
<td>The TREX can be configured using manual configuration or dynamic configuration in the XCM. When using Dynamic configuration, the values of the RFC destination to the IMS server are normally retrieved automatically from the underlying backend CRM system (if the value of the parameter “useDynConnParams”</td>
</tr>
</tbody>
</table>

**Network Security**

For information on network security refer to the top chapter Network Security and to the CRM Operation Guide.
is "true"). When you choose this setting, you do not have to specify any other parameter for this component. The other possibility 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 web server or different web servers are able to access different IMS servers, thereby implementing web load balancing or high availability. The distribution and update management of the indexes between such different IMS servers must be performed by other mechanisms (E-Commerce does not provide support for this).

At present, no security level is set for both the configurations. After the implementation, the RFC connection between the TREX and the CRM system will be secured using SNC. We can also use other methods,
### Data Storage Security

The data storage security is explained as follows:

#### Cookies

Cookies store a small amount of data on the client browser. E-Commerce uses two types of cookies:

- **Session cookies**
  
  These cookies are required to keep a client session and are deleted when the browser is closed.

  ![Warning](image)

  We recommend you to keep session cookies turned on for both security and functional purposes.

- **Persistent cookies**

  These cookies are used to store data on the client machine. For information on the data which is stored in these cookies, refer to section Data Storage Security.

  ![Warning](image)

  If these cookies are disabled, this functionality will not work.

For information on how to control cookie handling, refer to 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 explained below:

- **B2C**

  The cookie stores the Business Partner GUID if a user logs on or registers and maintains his profile. As a result, in E-COMMERCE CRM, the personalized product recommendations offered to the user are also stored in the cookie if the user maintains the personal data.

- **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

Some data is stored in the database of the Web AS Java, such as:

**Order templates**

When using the Java Basket in B2B or B2C application, the data is stored in SAP Web AS database. All data regarding order templates and shopping baskets is stored in the database without payment information (Credit Card number).
**XCM Application Configuration Data**

The E-COMMERCE web application is configured using the XCM Administration tool. The customer settings are stored in the local database of the WebAS Java. Some data is encrypted using the Secure Storage service of the J2EE Engine before it is stored in the database. The password of the service user is an example of encrypted data.

Sensitive XCM data is only encrypted securely if you have installed the SAP Java Cryptographic Toolkit. It is strongly recommended to install the Cryptographic toolkit. If you have not installed the Cryptographic toolkit the data is just encoded using base 64 encoding. For Information how to install the Cryptographic Toolkit refer to SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → Information Integration → Knowledge Management → Administration Guide → Knowledge Management → Administration Guide → Security Configuration → Configuration of the TREX Security Settings → Using the Cryptography Tools.

If you intend to transport (copy) XCM configuration data from one J2EE Engine to an other J2EE Engine, you have also to copy the keys used to encrypt sensitive XCM data from one engine to the other engine. This is done in the key storage service of the J2EE Engine. The following procedure describes how you can copy a Secure Storage key:

- Logon to the J2EE Engine where XCM data has been encrypted
- Select the Key Storage service
- Since you can only export complete views, we will create a temporary view for exporting the keys. Create a new view e.g. ‘xcmkeycopy’
- In the next step import (button Import from Other) the needed keys from the secure storage view into the newly created view. Every web application has an own key. Select the keys for the web applications you would like to transport the XCM data
- Save the xcmkeycopy view to file
- Log on to the engine you would like to import the keys and select the Key Storage service
- Import the previously exported keys in the secure storage view

**Security for Additional Applications**

For information on the security aspects of the other components used in an E-Commerce scenario, refer to the corresponding Security Guides.

**Other Security-Relevant Information**

**Java Script**

The E-Commerce applications use Java Script extensively. If Java Script is disabled on the browser, the application will not work as expected.

**Restricting Access to technical Administrator of E-Commerce applications**

Every E-Commerce web application has some pages used for technical administration of the web application.

In addition to the other features, the administration area provides following features:

- Application configuration for example, connection parameter to CRM or ERP by using Extended Configuration (XCM) Administrator tool
• Overview on various caches

For more information about the different features of the administration area, refer to the Configuration Information in the Solution Manager of the corresponding web application (e.g. b2b for ERP or CRM). For information about XCM, refer to the E-Commerce Installation Guides on the SAP Services Marketplace under service.sap.com/crm-inst.

You can access the administration pages as follows: http://host:port/<app name>/admin, e.g. http://localhost:50000/b2b/admin

It is mandatory to restrict access to the application administration pages from the Internet. This should be done by a HTTP proxy or an Reverse proxy. If you do not have such a proxy you have to turn off the Administration pages completely.

The following figure depicts the way how to protect the administration pages

- From the internet: No access at all
- From the intranet: Access is secured using basic authentication

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, refer to the Checklists section
Restricting Access to E-COMMERCE Administration pages from the Intranet

The administration pages are secured using Basic Authentication. This ensures that you have to provide the username and password before you can access the application.

Only users being part of the isaadmin role have access to the administration pages. After the assigned to this role. The user Administrator is always part of administrators the group.

We recommend you to not use the Administrator user for administering the web application. The administrator of the web application should have less rights than the administrator of the J2EE Engine (e.g. should not be able to shut down the J2EE Engine).

Instead of using the J2EE Administrator, a new user, such as ecommerceadmin should be created and assigned to the isaadmin role.

The following steps describe how to create a new user on the SAP J2EE Engine. For details, see the SAP Help Portal under help.sap.com □ Documentation □ SAP NetWeaver □ SAP NetWeaver □ SAP NetWeaver □ SAP NetWeaver Configuration □ SAP Web Application Server □ SAP Web Application Server (Java) □ J2EE engine Configuration:

1. Log on to the J2EE Engine by using Visual Administrator using
2. Select the Security Provider Service of the J2EE Server.
3. Select the User Management tab pane.
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. Select the Policy Configurations tab pane.
9. Select the E-COMMERCE for which you the user will be the administrator, for example, sap.com/crm.b2b"b2b.
10. Click the Security Roles pane
11. Select the isaadmin role.
12. Assign the previously created user to the role.

Restricting Access to E-COMMERCE Administration pages from the Internet

As a general rule, define as few mappings as possible. The HTTP server should allow those requests that are required by your application. All other request must be blocked.

In order to prevent access to the E-Commerce administration perform the following steps:

- Using IIS HTTP Server in front of J2EE Engine
  You have an HTTP server between the J2EE Engine and the Internet that is recommended by the CRM Operation Guide. It is important to restrict access through the web server for the following pages:
  
  
  `<applicationname>/admin`. 

  You can restrict access by using the IIsisProxy, for example:
<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>
      <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>
      <compress-types>text/html, text/plain</compress-types>
    </target>
  </mapping>
</ISAPI-config>

The mapping to the E-COMMERCE Administration leads to a non-existing area /error.

- **Using Apache HTTP Server in front of J2EE Engine**

  The security relevant settings of the Apache HTTP server are not explained here. Refer to:
  - Example of a configuration

    # 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 the J2EE Engine
  You must turn off all the features of administration. Refer to the Turning Features of Administration Area Off section.
  Please check if the mappings are correct by performing a security check as described in the checklist.

**Turning Features of Administration Area Off**

You can turn on/off access to each feature of the administration area by using the following context parameter in the web.xml:

adminconfig.core.isa.sapmarkets.com

If you have restricted access to the administration pages by using HTTP mappings as described in the previous section, you normally do not need to use this feature. However, if you access the application directly from the Internet by using the HTTP server within the J2EE engine, we recommend you to follow the instructions in this section.

The value of this parameter contains a comma-separated list of keywords. Each key word 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 SAP J2EE Engine Visual Administrator in the Service WebContainer:

1. Log on to the J2EE Engine by using Visual Administrator.
2. Select the WebContainer Service of the J2EE Server.
3. Select the required web application.
4. Click View; A new panel opens.
5. Select Context Parameters tab pane.
6. Select the adminconfig.core.isa.sapmarkets.com context parameter.
7. Change the setting.
8. Press the Modify button.

After changing the settings, you must restart the web application. This is performed in the deploy service. It is recommended to disable ALL administrative features by removing the value from the adminconfig.core.isa.sapmarkets.com context parameter.

The following table provides an overview of the available features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Access after Installation (not all web applications support all settings mentioned in this table)</th>
</tr>
</thead>
<tbody>
<tr>
<td>isacorecache</td>
<td>Application core caches</td>
<td>Yes</td>
</tr>
<tr>
<td>catalogcache</td>
<td>Web catalog cache</td>
<td>Yes</td>
</tr>
<tr>
<td>corecache</td>
<td>System level cache</td>
<td>Yes</td>
</tr>
<tr>
<td>jcoinfo</td>
<td>Information about SAP Java Connector</td>
<td>Yes</td>
</tr>
<tr>
<td>logging</td>
<td>This feature is not longer supported in CRM 5.0 and is kept for backward compatibility. Logging is now configured centrally in the J2EE Engine (see CRM Configuration Guide about E-Commerce logging and documentation on Visual Administrator how to configure logging)</td>
<td>Yes</td>
</tr>
<tr>
<td>version</td>
<td>This feature is not longer supported in CRM 5.0 and is kept for backward compatibility. Please refer to the CRM Operation Guide how to get version information of a E-Commerce application</td>
<td>Yes</td>
</tr>
<tr>
<td>xcmadmin</td>
<td>Turns access to XCM Administration tool on/off</td>
<td>Yes</td>
</tr>
<tr>
<td>ccmshheartbeat</td>
<td>Heatbeat configuration. See CRM Operation Guide on further information on E-Commerce supportability</td>
<td>Yes</td>
</tr>
<tr>
<td>dbmig</td>
<td>Controls whether migration tool for 4.0 shop data into 5.0 database is turned on.</td>
<td>Yes</td>
</tr>
<tr>
<td>scheduler</td>
<td>Controls whether schedule</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Some Administration features are controlled by XCM

**Administration features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Access after Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>appinfo</td>
<td>This feature is controlled in XCM Administrator under:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>General Settings → Customer → &lt;application name, for example, b2b&gt; → &lt;application name&gt;config → appinfo</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This feature must be turned off in production.</td>
<td></td>
</tr>
<tr>
<td>show.start.jsp</td>
<td>A list of available XCM configurations is presented when starting the application like this http://&lt;host&gt;:&lt;port&gt;/&lt;application name e.g. b2b&gt;/</td>
<td>No</td>
</tr>
<tr>
<td>show.start.jsp</td>
<td>General Settings → Customer → &lt;application name, for example, b2b&gt; → &lt;application name&gt;config → showStartPage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This feature must be turned off in production.</td>
<td></td>
</tr>
<tr>
<td>sat</td>
<td>Specifies whether Single Activity Trace is turned on. For further information see Solution Management Guide for mySAP CRM</td>
<td>No</td>
</tr>
</tbody>
</table>

**Disabling XCM Application Configurations**

XCM enables you to create multiple configurations of your E-Commerce application. You can even run different the application using different configuration at the same time.

You have to make sure to turn off or delete all not used application configurations in production environment in XCM.

For detailed information on usage the XCM tool refer to the Solution Manager Documentation

1. Start XCM of the web application
2. Press the button Edit
3. Select in the tree: Select start □ Application Configuration □ Customer □ <the configuration you do not want to use>
4. Deselect the 'active configuration' checkbox
5. Press the 'Save configuration' button
6. Perform steps 3 to 5 for every configuration not used in production environment
7. Click the 'Display' button to release lock on XCM configuration

**Encryption of payment cards**

In the E-Commerce B2B and B2C application it is possible using the payment form payment cards. For data protection reasons it will be recommended to store the payment card number encrypted on the database. Please follow the corresponding instructions of the configuration documentation of the Solution Manager to enable the encryption of payment card numbers.

**Trace and Log Files**

In contrast to previous versions of E-Commerce logging/tracing is now configured centrally using the Log Configuration Service of the J2EE Engine. The service is configured using the Visual Administrator tool of the J2EE Engine.

Make sure that the severity level for the following locations is set to ERROR:
- com.sap.isa
- com.sap.eservice

**Session Trace**

E-Commerce application support a so called single session trace. This trace is used to get the full trace information for a particular session. This function is usually used by developers (e.g. in customer projects) or by support personnel. The trace can be turned on like this

- Open the start page of the web application
  
  \[http://<server>:<port>/<application name e.g. b2b>\]

  The page has to be turned on (XCM Start → Customer → <web application name e.g. b2b> → showStartPage (true))
- Click on the 'Single Session Trace' of the application configuration you would like to trace

All trace information related to the session is written into the default trace of the WebAS Java and can be viewed with the LogViewer

The trace also traces the whole HTTP based communication e.g. passwords, credit card numbers) between the web client and J2EE engine. If you want to make sure that no one else can see this information you have to delete the default traces of the WebAs 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 SAP E-Commerce Administration pages/functions**

<table>
<thead>
<tr>
<th>Security Item</th>
<th>Method</th>
<th>Reference</th>
<th>Result/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check if access to the SAP E-COMMERCE administration area is restricted from the Intranet.</td>
<td>Call admin area from the intranet, for example: <a href="http://host:port/b2b/admin">http://host:port/b2b/admin</a></td>
<td>see chapter Creating a user for administration</td>
<td>A logon pop up must appear. Login using the user created during E-COMMERCE installation.</td>
</tr>
</tbody>
</table>
Log on using the user created during SAP E-COMMERCE installation

<table>
<thead>
<tr>
<th><strong>Check access to the administration are from the Internet. (if your application is exposed to the internet)</strong></th>
<th><strong>Call admin area from the internet, for example:</strong></th>
<th><strong>see chapter Restricting Access to technical Administrator of E-Commerce applications</strong></th>
<th><strong>A logon pop up must not appear. The http proxy must not forward the request to the /admin area.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.acme.com/b2b/admin">http://www.acme.com/b2b/admin</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Check if the Administrator password is blank</strong></th>
<th><strong>Call admin area from the intranet, for example:</strong></th>
<th><strong>You must not be able to logon.</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://host:port/b2b/admin">http://host:port/b2b/admin</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User – Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password – leave empty</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Check if appinfo feature is turned off. This feature must be turned On only during development.</strong></th>
<th><strong>Call application with additional appinfo request parameter, for example:</strong></th>
<th><strong>You must not be prompted to logon. A second browser window that provides system information must not be opened.</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://host:port/b2b/b2b/init.do?appinfo=true">http://host:port/b2b/b2b/init.do?appinfo=true</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>See chapter Turning Features of Administration Area Off</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Ensure that the showstacktrace switch is turned off</strong></th>
<th><strong>Check in XCM – component UI value showstacktrace. isacore assigned to the application configuration you are using</strong></th>
<th><strong>The value must be false.</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Disable or delete all not needed XCM configurations</strong></th>
<th><strong>Disable or delete all XCM configuration not used in production</strong></th>
<th><strong>All disabled configurations are marked with a red light in the XCM tree</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Make sure that HTTP based file browsing is turned off</strong></th>
<th><strong>Call the application like this</strong></th>
<th><strong>SAP Note 531495</strong></th>
<th><strong>You must not see a directory content.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://host:port/b2b/b2b">http://host:port/b2b/b2b</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Protecting IPC Price Analysis Tool

<table>
<thead>
<tr>
<th><strong>Security Item</strong></th>
<th><strong>Method</strong></th>
<th><strong>Reference</strong></th>
<th><strong>Result/Comments</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that IPC price analysis and enable pricing conditions display is turned off.</td>
<td>Check in XCM – component ui value enable.priceAnalysis</td>
<td></td>
<td>The value must be false.</td>
</tr>
</tbody>
</table>

### Protecting E-Commerce Administration pages/functions

<table>
<thead>
<tr>
<th><strong>Security Item</strong></th>
<th><strong>Method</strong></th>
<th><strong>Reference</strong></th>
<th><strong>Result/Comments</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice over IP in Web collaboration uses the NetMeeting Active X control</td>
<td>See SAP Note 725954</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
E-Service

Introduction
E-Service application is an E-Commerce scenario. For more information, refer to E-Commerce corresponding chapters.

Why Is Security Necessary?
Refer to E-Commerce corresponding chapter for more information.

Technical System Landscape
The following graphic shows the components that are required for the SAP Internet Customer Self-Service (ICSS) Java Application.

User Administration and Authentication

User Management
The ICSS application runs using the SU01 user type and provides its service to any SU01 user connected to a business partner.

For Complaints & Returns and Remanufacture Inspection applications, refer to E-Commerce corresponding chapter.

User Management Tools
Tool | Detailed Description | Prerequisites
--- | --- | ---
SU01 Transaction | Refer to SU01 documentation |  
Web AS Java user management using the Visual Administrator | Refer to User Management Tools for all E-Commerce Scenarios |  

**User Types**

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM</td>
<td>Anonymous user for stateless connection</td>
<td>No</td>
<td>SU01 service user</td>
<td>No</td>
<td>SU01 user for establishing the stateless connection between CRM and ICSS</td>
</tr>
</tbody>
</table>

Refer to [E-Commerce Seite 107](#) User Types section for additional users.

**User Data Synchronization**
The data is only stored in the CRM system. As a result, no data synchronization occurs.

**Integration IntoSingle Sign-On Environments**
The application supports Single Sign-On through the SAP Enterprise Portal.

It only accepts SAP logon tickets.

**Authorizations**
The following table lists the authorization objects that are used in ICSS to provide minimum authorizations to users and prevent unauthorized access to the application or a part of the application.

The anonymous user is used in B2C scenario to provide access to functionality not requiring password protection like FAQ and Solution Search. This kind of user is not authorized to accessing other sensitive functions and therefore it is recommended to restrict its access.

**Delivered Roles**

<table>
<thead>
<tr>
<th>Delivered role</th>
<th>Scenario</th>
<th>Auth. Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----------------------------</td>
<td>-----</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>SAP_CRM_COCO_ECO_ISE_WU_B2C</td>
<td>B2C</td>
<td>B_BUPA_RLT</td>
<td>Internet user</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISE_TU_B2C</td>
<td>B2C</td>
<td>S_RFC:</td>
<td>Service user role</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----</td>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTVT=Execute</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RFC_NAME=*</td>
<td></td>
</tr>
</tbody>
</table>

B_USERSTAT  
B_USERST_T  
B_BUPR_BZT:  
  RELTYP=BUR001  
COM_PRD  
COM_CAT  
COM_PRD_CT  
COM_ASET  
COM_IL  
CRM_CMP  
CRM_ORD_LP  
CRM_ORD_OP  
CRM_SEO  
CRM_CO_SE  
CRM_Isa_pl:  
  ACTVT=READ (33)  
CRM_ISE_SS  
PLOG  
S_RFC  
S_USER_SYS  
S_ALV_LAYO  
S_PRO_AUTH  
S_TABU_DIS  
S_BTCH_ADM  
S_BTCH_JOB  
S_OC_DOC  
S_OC_FOLCR  
S_OC_ROLE  
S_OC_SEND  
S_CTS_ADMI  
S_USER_GRP  
S_DEVELOP:  
  OBJTYPE=DEBUG  
CRM_TXT_ID (for Item text)  
S_TCODE for Work force management  

role
The following table lists the RFCs that are used in Complaints & Returns and Remanufacture Inspection to provide minimum authorizations to users and prevent unauthorized access to the application or a part of the application.

### Authorization Objects

<table>
<thead>
<tr>
<th>Delivered role</th>
<th>Scenario</th>
<th>Auth. Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_ECO_ISE_WU_CR</td>
<td>B2B</td>
<td></td>
<td>Internet user role</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISE_TU_CR</td>
<td>B2B</td>
<td></td>
<td>Service user role</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISE_WU_INSP</td>
<td>B2B</td>
<td></td>
<td>Internet user role</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISE_TU_INSP</td>
<td>B2B</td>
<td></td>
<td>Service user role</td>
</tr>
</tbody>
</table>

Refer to E-Commerce [Seite 107] Authorizations chapter for more information.

### Network and Communication Security

Refer to E-Commerce [Seite 107].

### Data Storage Security

The application data is stored in the SAP CRM system and can be accessed through the web browser.

- No persistent cookies are used.
- No data is stored on the client side.

Refer to E-Commerce [Seite 107] XCM Application Configuration Data sub chapter for more information.

### Other Security-Relevant Information

Refer to E-Commerce [Seite 107] Security-Relevant Information chapter.

### Trace and Log Files

Refer to E-Commerce [Seite 107] Trace and Log Files chapter.
Checklist
Refer to E-Commerce [Seite 107] Checklist.
Payment Cards Encryption

Introduction
Payment cards frequently replace cash as a means of payment, becoming indispensable to customers and valuable tools for businesses. The importance of payment cards requires their integration into business processes.

Payment card data can be entered in the following applications:

- Business Partner master data
- CRM Online
- E-Commerce Business-to-Business (B2B)
- Business-on-Behalf (BOB)
- E-Commerce Business-to-Consumer (B2C)
- Collaborative Showroom (CSR)

The data is filled into the payment form (for example credit card number) of sales order documents and can be stored in the PCA master in encrypted form. In the E-Commerce Hosted Order Management (HOM) application payment card data will be displayed if maintained by consumers in the CSR application.

In online transactions payment card can be displayed in masked (like 41111********11) or unmasked (full number, like 4111111111111111) form.

Relevant Security Guides

Important SAP Notes
The following table lists the most important SAP Notes for Payment Card Encryption.

<table>
<thead>
<tr>
<th>SAP Note</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>633462</td>
<td>Encrypt payment cards</td>
<td></td>
</tr>
<tr>
<td>597059</td>
<td>License conditions SAP Cryptographic Library</td>
<td></td>
</tr>
<tr>
<td>397175</td>
<td>SAP Cryptographic Software - Export check</td>
<td></td>
</tr>
<tr>
<td>662340</td>
<td>SSF Encryption Using the SAPCryptolib</td>
<td></td>
</tr>
<tr>
<td>890512</td>
<td>Visible Payment Card Numbers on BDOC Monitor</td>
<td></td>
</tr>
</tbody>
</table>
Technical System Landscape

To use the payment card encryption you have to do some preparations, as described in the following:

1. Install the SAPCrytoLib on all application server according SAP Note 662340
2. Call transaction STRUST
3. Create PSE for “Standard Application” and set algorithm to RSA and recommended key length to 1024.
4. Within the transaction STRUST create a backup of the PSE by PSE → Export

Authorization

- If you need to decrypt the payment card numbers, you need a user with the following authorizations:
  Authorization object B_CARD_SEC enables you to decrypt and to delete an entry.
  We recommend to give this authorization only to few persons in your company or department.
- If you want to create an order (One order API) e. g. in CRM you need the authorization object CRM_ORD_PC with the activities “display” and “change”

The masking functionality depends on activation of card encryption. If card encryption is active, in online transactions card number is shown always in masked form (after first save). In the E-Commerce scenarios the masking of payment cards depends on the current user authorizations. If an user has the authorization to decrypt payment card numbers (B_CARD_SEC) any card number will be displayed unmasked in the web applications.

If card encryption is inactive, card number appearance depends on the user authorizations of object CRM_ORD_PC.

Authorization

<table>
<thead>
<tr>
<th>ACTVT “02” Change</th>
<th>ACTVT “03” Display</th>
<th>Functionality in online transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>+</td>
<td>User can change payment card and the card number is shown completely (unmasked)</td>
</tr>
<tr>
<td>+</td>
<td>-</td>
<td>User can change payment card, but after saving the card number is shown in masked form</td>
</tr>
<tr>
<td>-</td>
<td>+</td>
<td>User can not change payment card, but can see the number in unmasked form</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>User can not change payment card and the card is shown in masked form</td>
</tr>
</tbody>
</table>

During data exchange process between CRM and ERP, payment card is decrypted before sending from CRM to ERP. For this reasons, if payment card encryption is active, usage of
separated user for processing MW flow is strictly recommended. In comparison to online user, this user should have full authorization of object B_CARD_SEC.

**Network and Communication Security**

**Communication Channel Security**
Within the People-Centric UI we recommend to use HTTPS encryption to protect the data. For the SAP GUI we recommend SNC encryption.

Please, pay attention that during data exchange process, card number is decrypted in CRM, and sent into ERP in decrypted form. Afterwards it can be encrypted again in ERP depending on the customizing settings. So, it is important to setup network encryption (RFC Connection between CRM and ERP).

**Communication Destinations**
If you want to send out decrypted payment card numbers, we recommend to use SNC encryption.

**Data Storage Security**
If you use payment card encryption it is encrypted with the SAP Cryptographic Library and forwarded to the database.

With the customizing the numbers of all kinds of payments cards are encrypted.

In case of data exchange of business transactions with ERP Backend, encryption is supported as well. Payment cards can be encrypted in both systems, or only in one CRM or ERP, or nowhere. In CRM if the encryption is active, card number is stored internally in BDoc (required for data exchange) in encrypted form as well.

For more information about Payment Card encryption in SAP ERP, refer to SAP Notes: 766703, 633462.

**Encryption prerequisite**
Payment card numbers are only encrypted if the ‘SAPCryptolib’ is installed on each application server. For more information regarding the installation and configuration of the ‘SAPCryptolib’ see SAP Note 662340.

Additionally a PSE for the “Standard Application” must be created using the ‘Trust Manager’ (transaction STRUST). The algorithm RSA must be selected for this entry.

**Data protection**
Due to the protection of privacy we recommend to store the payment card number encrypted on the data base. Furthermore any card number should be masked if it is presented in the user interface or printed out on documents.

**Other Security-relevant Information**
Take also in consideration which encryption software you will use.

You can use the SAPCryptolib for free. This library uses the encryption Standard PKCS7. Because of export regulations every customer has to download the library from SAP Service Marketplace under service.sap.com.

For more information concerning software, license determinations and download see the SAP Note 597059.
Checklist

Here you find a checklist with the features, their security settings and how you can prove them.

### Checklist

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption is activated</td>
<td>Use the transaction STRUST.</td>
<td>Shows whether SAPCryptolib is installed and the PSE is available on all servers.</td>
</tr>
<tr>
<td></td>
<td>Choose Environment → Display SSF Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the PSE is installed all traffic lights under Standard Application are green.</td>
<td></td>
</tr>
<tr>
<td>Test-Transaction</td>
<td>Are all data encrypted?</td>
<td>You can check the encryption over all servers with the transaction PCA_SC.</td>
</tr>
<tr>
<td>Encryption is active for all kinds of payment cards.</td>
<td>Choose in the implementation guide under Cross-Application Components → Payment Cards → Basic Settings → Maintain Payment Card Type</td>
<td>Check, whether the flag for encryption is set or not.</td>
</tr>
<tr>
<td>Payment card encryption is active</td>
<td>Check “change” authorization of online transactions</td>
<td>Authorization object CRM_ORD_PC</td>
</tr>
<tr>
<td></td>
<td>Authorization of system user used for MW flow processing</td>
<td>Required full authorization for object B_CARD_SEC</td>
</tr>
</tbody>
</table>
Selling via eBay

Introduction

Selling via eBay (SVE) consists of ABAP-based functionality on a SAP CRM or SAP ERP server and Java-based functionality on the Java stack of SAP NetWeaver (J2EE Engine). The user interface (UI) is provided by a Java-based application running on J2EE. This UI is exposed only in the intranet, though you can configure it to be available for Internet. The SVE application on the J2EE Engine communicates with the eBay server via the Internet. Since SVE stores and communicates customer-specific and seller-specific information, it is essential to protect your SVE application.

The security aspects of this application depend primarily on the security aspects associated with SAP Internet Sales (CRM).

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver</td>
<td>SAP NetWeaver security guide</td>
<td>Configuring the Use of SSL on the SAP J2EE Engine [Extern]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring SNC (SAP J2EE Engine -&gt; ABAP Engine) [Extern]</td>
</tr>
<tr>
<td>E-Commerce [Seite 107]</td>
<td>SAP Customer Relationship Management (CRM) security guide</td>
<td>• User Administration and Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authorizations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network and Communication Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Storage Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other Security-Relevant Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trace and Log Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Appendix</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

The SVE application runs in the intranet. However, it communicates with the eBay API server on the Internet via HTTPS/SSL. This communication can contain buyers’ personal details and sellers’ authentication information. eBay APIs (such as publishing an item for auction on eBay) are XML documents containing information about the item and seller authentication. The seller authentication information includes the eBay seller tokens along with the eBay authentication certificates.

The SVE application must be secured to prevent unauthorized access to:

- Data packets being exchanged between the SVE and eBay API server, and thereby to buyers’ personal information
- Information when communication is not encrypted

User IDs and passwords to communicate with the CRM or ERP system also need to be secured.
Important SAP Notes

Check regularly which SAP Notes are available about the security of the application.

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>828420</td>
<td>CRM E-Commerce Composite Security Note</td>
<td>Central entry point for current information on CRM E-Commerce. Please check this note regularly.</td>
</tr>
</tbody>
</table>

User Administration and Authentication

User administration is required for:

- J2EE deployed SVE administration (XCM and other J2EE administration)
- Auction seller and auction administrator account management on the ERP system and CRM system
  The auction seller and auction administrator must be SU01 users and have the authorizations stated in Authorizations (see below).
- eBay seller administration
  eBay seller accounts must be created on the eBay site. These eBay user accounts are mapped with ERP or CRM accounts in SVE using the SVE administration UI. You can access the SVE user administration UI using the following URL: http://servername:port/sve/init.do

User Management

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>J2EE Engine user management using Visual Administrator</td>
<td>Access to administration pages is controlled using J2EE Engine security. Automatically activated after deploying SVE.</td>
</tr>
<tr>
<td>User management for ABAP engine (transaction SU01) Maintenance of roles and profiles (transaction PFCG)</td>
<td>In transaction SU01, choose Help → Application Help. For information about the different user types, see the configuration information for SVE in SAP Solution Manager.</td>
</tr>
<tr>
<td>(CRM only) Business partner maintenance (transaction BP)</td>
<td>See Creating Business Partner Master Data in the CRM System, which you can find on SAP Help Portal under mySAP Customer Relationship Management.</td>
</tr>
</tbody>
</table>
User Types

In the SAP CRM security guide, see E-Commerce [Seite 107] → User Types. In addition, the following user types exist in SVE.

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERP and CRM system</td>
<td>Anonymous user for stateless connection</td>
<td>No</td>
<td>SU01 service user</td>
<td>No</td>
<td>SU01 user for establishing stateless connection between ERP or CRM and SVE system.</td>
</tr>
<tr>
<td>ERP and CRM system</td>
<td>SVE seller or administrator</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>User that logs into SVE. Full state SVE connection is established with it. Sales documents are created using this connection.</td>
</tr>
<tr>
<td>eBay</td>
<td>Seller user in eBay</td>
<td>No</td>
<td>None</td>
<td>No</td>
<td>Seller must be created in external (non-SAP) eBay system. Auctions published on eBay are associated with this seller user ID. eBay seller ID is mapped to seller in ERP or CRM system via eBay administration UI. See configuration information for SVE in SAP Solution Manager.</td>
</tr>
</tbody>
</table>

User Data Synchronization

No user data synchronization is required for SVE.

Logon Process

SVE supports SAP logon tickets (transaction SSO2). If SAP User Management Engine (UME) is enabled, further logon methods are available such as X.509 digital certificates. For more information, see the UME documentation on SAP Help Portal. In the SAP CRM security guide, see also E-Commerce [Seite 107] → Logon Process.
Authorizations

In the SAP CRM security guide, see E-Commerce [Seite 107] → Authorizations.

The following roles are delivered with the appropriate authorizations for SVE. We recommend using these roles because they provide the minimum authorization for each user type. To assign the role to a user in the CRM or ERP system, use transaction PFCG.

<table>
<thead>
<tr>
<th>User</th>
<th>CRM Role</th>
<th>ERP Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous user for stateless connection</td>
<td>SAP_CRM_ECO_TU_SVE</td>
<td>SAP_ECO_TU_SVE</td>
<td>Handles background tasks like auction winner determination</td>
</tr>
<tr>
<td>Auction seller</td>
<td>SAP_CRM_ECO_SVE_WU_SELLER</td>
<td>SAP_ECO_SVE_WU_SELLER</td>
<td>Creates and posts auctions on eBay</td>
</tr>
<tr>
<td>Auction administrator</td>
<td>SAP_CRM_ECO_SVE_WU_ADMIN</td>
<td>SAP_ECO_SVE_WU_ADMIN</td>
<td>Administers auction seller accounts such as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Setting validity dates for sellers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Binding eBay users with ERP or CRM system</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Scheduling tasks that communicate with eBay</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Maintaining themes and other standard settings</td>
</tr>
</tbody>
</table>
### Network and Communication Security

#### Communication Channel Security

![Diagram illustrating network and communication security](image)

**Selling via eBay Communication Channels**

#### Communication Channels and Protocols Used Between Different Components

<table>
<thead>
<tr>
<th>Component A</th>
<th>Component B</th>
<th>Channel</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>HTTP server</td>
<td>Front end to server</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication with Web browser</td>
<td></td>
</tr>
<tr>
<td>HTTP server</td>
<td>J2EE Engine/SVE Web application</td>
<td>Server to server</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requests from Web browser are forwarded to SVE application running on J2EE engine. Responses from SVE are forwarded to Web browser.</td>
<td></td>
</tr>
<tr>
<td>J2EE Engine/SVE</td>
<td>eBay API server</td>
<td>SVE to eBay external API server</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SVE communicates with eBay server in Internet via HTTPS. SVE application contains inbuilt HTTPS client that communicates with eBay API server.</td>
<td></td>
</tr>
<tr>
<td>J2EE Engine/SVE</td>
<td>CRM or ERP system</td>
<td>Application to server</td>
<td>RFC/SNC</td>
</tr>
</tbody>
</table>
Web application

Java-based SVE application executes application logic running on SAP system.

J2EE Engine/SVE Web application

Database (SQL server)

Application to server
Stores eBay information such as user mappings, auction information.

JDBC

For information about how to protect each communication channel, see the SAP CRM security guide → E-Commerce [Seite 107] → Communication Channel Security.

For information on how to configure the J2EE Engine with SSL, see Configuring the Use of SSL on the SAP J2EE Engine [Extern], which you can find on the SAP Help Portal under SAP NetWeaver.

**Communication Destinations**

**Connection Destinations from SVE**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to CRM/SAP system</td>
<td>No</td>
<td>RFC</td>
<td>See Authorizations above</td>
<td>Technical user for stateless (anonymous) communication with back-end system. Configured using XCM tool after installation.</td>
</tr>
<tr>
<td>Connection to eBay API server</td>
<td>No</td>
<td>HTTPS</td>
<td>No</td>
<td>Configured using XCM tool after installation. See configuration information for SVE in SAP Solution Manager.</td>
</tr>
</tbody>
</table>

**Data Storage Security**

Confidential application data such as user IDs, passwords, and eBay authentication tokens is stored in J2EE secure storage instead of the database. In addition, the other JCo passwords to communicate with the ERP or CRM system are stored in secure storage. To use secure storage, you must install the SAP Web AS Java cryptographic toolkit. You can configure the encryption levels in secure storage. For more information, see the SAP NetWeaver security guide.

In the SAP CRM security guide, see also E-Commerce [Seite 107] → Data Storage Security.

**Other Security-Relevant Information**

In the SAP CRM security guide, see E-Commerce [Seite 107] → Other Security-Relevant Information.

SVE Administrator Area
The SVE administrator has the privileges explained in Authorizations above. To restrict access to the SVE administrator area, assign the user to the administrator role specified in Authorizations.

**Trace and Log Files**

In the SAP CRM security guide, see E-Commerce [Seite 107] → Trace and Log Files.

**Appendix**

**Checklists**

In the SAP CRM security guide, see E-Commerce [Seite 107] → Checklists.

<table>
<thead>
<tr>
<th>Security Item</th>
<th>Method</th>
<th>Reference</th>
<th>Result/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect SVE administration pages/functions</td>
<td>For protecting Internet Sales administration pages/functions, see the SAP CRM security guide → E-Commerce [Seite 107] → Checklists</td>
<td>All items in this checklist should be addressed</td>
<td></td>
</tr>
<tr>
<td>Install SAP Web AS Java cryptographic toolkit</td>
<td>See Transport Layer Security on the SAP J2EE Engine [Extern], which you can find on SAP Help Portal under SAP NetWeaver</td>
<td>All sensitive information used in SVE is stored in secure storage. Also, communication between J2EE and eBay API server is secured.</td>
<td></td>
</tr>
</tbody>
</table>
SAP Internet Pricing and Configurator

Introduction

This section provides information about the security aspects of the Internet Pricing and Configurator (IPC) web-application running in the CRM scenario.

The security relevant topics of the dependent components, such as the J2EE Engine, are described in detail in the corresponding security guides. For more information, see E-Commerce [Seite 107].

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPC Web Application</td>
<td>Refer to the chapter on SAP Internet Sales in this guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data storage Security - For XCM customer configuration data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other Security-Relevant Information - For Internet Sales Administrator Area</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trace and Log files</td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td>J2EE Guide</td>
<td>How to configure SSL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>How to install SNC</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

The IPC web-application communicates over the network with the CRM system using RFC. Therefore the communication must be secured to prevent that someone can spy-out this communication to get e. g. account credentials, passwords or content. See section Network and Communication Security [Seite 39].

Furthermore the IPC web-application provides features for the convenience of the user that could be regarded as insecure in some scenarios. For example: Import/Export functionality can reveal unwanted information to the user. That is ok in an in-house scenario but could be considered as security-relevant if the IPC web-application is used as part of an application accessible via the Internet (e.g. as part of Internet Sales B2C).

All security-relevant features can be turned off by one single switch: the IPC Security Level. The following table explains the different security levels and their impacts on the IPC web-application:

IPC Security Levels

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>All features of the web-applications are enabled.</td>
</tr>
<tr>
<td>1</td>
<td>Secure Mode (Default)</td>
</tr>
<tr>
<td></td>
<td>Features considered as insecure are disabled.</td>
</tr>
<tr>
<td></td>
<td>The following features are disabled:</td>
</tr>
<tr>
<td></td>
<td>Import/Export of configuration data to the local client.</td>
</tr>
</tbody>
</table>
The IPC Security Level is an XCM parameter that can be maintained using the XCM Administration tool. For setting XCM parameters, refer to IPC Configuration Support → Extended Configuration Management.

**Important SAP Notes**

⚠️ Check regularly which SAP Notes are available about the security of the application.

For information on general notes related to the E-Commerce scenario, see E-Commerce [Seite 107].

**Important SAP Notes**

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>412309</td>
<td>Authorization profile RFC user for IPC</td>
<td>Restrictions the authorization rights for RFC connections from IPC Server to CRM</td>
</tr>
<tr>
<td>828420</td>
<td>CRM E-Commerce composite security note.</td>
<td>This note is the central entry point for up to date information on CRM E-Commerce. Therefore, check this note regularly.</td>
</tr>
</tbody>
</table>

**User Administration and Authentication**

The administration of users is required in the following areas:

- J2EE deployed IPC administration (XCM and other J2EE admin)
  
  Refer to the the User Administration and Authentication section in E-Commerce document.

- CRM Backend-User for IPC web-application
  
  The CRM Backend-User is used by the IPC web-application to connect to the CRM backend-system. It must be of SU01 user type with a profile attached to it. This profile can be created in CRM through the transaction PFCG. In XCM administration tool the credentials have to be maintained. For authorizations refer to subsection Authorizations under this section.

**User Management**

**User Management Tools**

Refer to User Management Tools for all ISA scenarios in the corresponding section in the E-Commerce [Seite 107].

**User Types**

See corresponding section in E-Commerce [Seite 107] for information common for all E-Commerce applications.

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM</td>
<td>User, which is used by the IPC web application to connect to</td>
<td>No</td>
<td>SU01 service user</td>
<td>No</td>
<td>SU01 User for establishing the connection between CRM and IPC web-</td>
</tr>
</tbody>
</table>
User Data Synchronization

The synchronization of user data is not applicable as there are no individual users.

Integration Into Single Sign-On Environments

The integration into Single Sign–On environments is not applicable as there are no individual users.

Authorizations

See corresponding section in E-Commerce [Seite 107] for information common for all E-Commerce applications.

Authorizations

<table>
<thead>
<tr>
<th>User</th>
<th>Role</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backend-User</td>
<td>User that is used by IPC web-application</td>
<td>Create a profile for this role in CRM that uses the S_RFC authorization</td>
</tr>
<tr>
<td></td>
<td>to connect to the CRM.</td>
<td>object. See note 412309 on how to set up an appropriate role.</td>
</tr>
</tbody>
</table>

For the Backend-User that is used to connect to the CRM, a role must be created which includes authorization object S_RFC. Refer to note 412309. The following function groups must be included in the role:

- COM_CFG_API_ENGINE_COMMAND
- COM_CFG_API_UI_COMMAND
- CNV_UNITS
- CNV_CURRENCY
- SPC_DEPRECATED
- IPC_UI_CONFIG
- CRM_IPC_GRID_VMC_COMMANDS

Network and Communication Security

Communication Channel Security

The following Communication Channels and Protocols are used between different components:

| 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 | Server to server Requests from web browser are forwarded to IPC application running on J2EE engine. Responses from IPC are forwarded to the web browser. | HTTP/HTTPS (secure)
J2EE Engine/IPC web-application | CRM | Application to server Java based IPC application executes application logic running on the SAP system. | RFC/SNC (secure)

In most cases you have the option between a non-secure/secure protocol. The chapters Secure Socket Layer (SSL) and Secure Network Communication (SNC) from E-Commerce [Seite 107] give you the information to decide which protocol fulfils your security requirements: SSL or SNC.

**Network Security**

For network security, refer to the Network Security in the E-Commerce [Seite 107].

**Communication Destinations**

**Connection Destinations**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to CRM/SAP system</td>
<td>No</td>
<td>RFC</td>
<td>Refer to the Authorizations section.</td>
<td>Technical user used for communication with the backend system. Configured using XCM tool after installation.</td>
</tr>
</tbody>
</table>

**Data Storage Security**

No data is stored in the IPC web-application. The results of configuration and pricing are stored in the applications that call the IPC web-application.

IPC web-application stores only administration data. For more information refer to chapter Data Storage Security – XCM Application Configuration Data in E-Commerce [Seite 107].

A Web browser is required as the user interface. Session cookies (are deleted when closing the web browser) are used to keep a client session. The cookie does not store any other data. On the client side, no user data is stored. For more information see the chapter Data Storage Security – Cookies in E-Commerce [Seite 107].

**Security for Additional Applications**

Other components using the IPC applications
For information on how to secure the other components that use the IPC web-applications, refer to the corresponding Security Guides.

**Other Security-Relevant Information**

The IPC web-application uses the Java Script extensively. If Java Script is disabled on the browser, the application does not work. In addition, the application uses session cookies (are deleted when closing the web browser) to keep a client session. If the cookies are disabled, it is not guaranteed that the application will work correctly.

No persistent cookies are used.

For information on the web-based administration tool, see the chapter Other Security-Relevant Information – Restricting Access to technical Administrator of E-Commerce applications in E-Commerce [Seite 107].

**Trace and Log Files**

For information on Trace and Log files, refer to Trace and Log Files in E-Commerce [Seite 107].

**Checklist**

Here you find a checklist with the features, their security settings and how you can prove them.

For mandatory going live check list refer to E-Commerce [Seite 107].

### Checklist

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Commerce Administration Console</td>
<td>Call admin area:</td>
<td>All items mentioned in this checklist must be addressed.</td>
</tr>
<tr>
<td></td>
<td><a href="http://host:port/ipc/admin">http://host:port/ipc/admin</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Go through the checklist under</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protecting Internet Sales Administration pages/functions in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E-Commerce.</td>
<td></td>
</tr>
<tr>
<td>Knowledge Base Selection</td>
<td>Call knowledgebase selection:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://host:port/ipc/init.do?scenario.xcm=crmproductsimulation">http://host:port/ipc/init.do?scenario.xcm=crmproductsimulation</a></td>
<td></td>
</tr>
<tr>
<td>IPC Security Level</td>
<td>Check in XCM – component “security” value “security.level”</td>
<td>The value must be “1” (i.e. secure mode).</td>
</tr>
</tbody>
</table>
Interaction Center
Interaction Center WinClient

Introduction

The Interaction Center WinClient (application component CRM-CIC) is based on SAP Web Application Server (SAP Web AS) 6.40 and SAP CRM 5.0.

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow Management</td>
<td>SAP Basis</td>
</tr>
<tr>
<td>SAP Web Application Server</td>
<td>SAP Web Application Server Security Guide</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

The Interaction Center (IC) WinClient normally runs in an intranet. Security is necessary because the IC WinClient:

- Connects to communication management software to obtain data from incoming calls; this data can include personal information and sales order information
- Accesses data in the CRM system, such as business partner information

Therefore, it is very important to restrict access to this data.

Important SAP Notes

![Warning]

Check regularly which SAP Notes are available about the security of the application.
Technical System Landscape

Typical Landscape of Interaction Center WinClient

The CRM Server includes the Interaction Center (IC) WinClient framework and the following SAP applications:

- SAPphone
  SAPphone provides a telephony function to the IC. It allows data to be exchanged between the CRM Server and the telephony component.

- SAPconnect
  SAPconnect provides an integrated e-mail function to the IC. It enables communication management software [Extern] to connect to the SAP system (for example, an e-mail server or SMTP server).

User Administration and Authentication

User Management

The IC WinClient uses standard user management tools to maintain users. See the following table:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User maintenance (transaction SU01)</td>
<td></td>
</tr>
</tbody>
</table>
Profile Generator (transaction PFCG)

You use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.

**User**

The following users must be created for the IC WinClient:

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory User who can access IC WinClient functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Created by CRM system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>WF-BATCH</td>
<td>Yes</td>
<td>System user</td>
<td>No</td>
<td>Mandatory User who can process background workflow tasks</td>
</tr>
<tr>
<td>ERP backend</td>
<td>End user</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory User who can access ERP background functions. Depending on RFC destination, user can be individual user or system RFC user. Created by ERP system administrator</td>
</tr>
<tr>
<td>BW user</td>
<td>End user</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Optional Created by BW system administrator if you want to evaluate interactive scripting through BW reporting</td>
</tr>
</tbody>
</table>

**User Data Synchronization**

Data Synchronization Between CRM System and Other Systems
### Data Exchanged

<table>
<thead>
<tr>
<th>Data Exchanged</th>
<th>When Synchronized</th>
<th>How Synchronized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business partner data</td>
<td>When business partner is created in CRM, the data is replicated to ERP.</td>
<td>Automatically by CRM middleware settings</td>
</tr>
<tr>
<td></td>
<td>When business partner is created in ERP, the data is replicated to CRM.</td>
<td></td>
</tr>
<tr>
<td>Call related information between SAPphone and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>communication management software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data between CRM and third-party communication</td>
<td>If you want to use the predict call functionality, call list data is replicated</td>
<td>Synchronize when managing the call list to predict calls</td>
</tr>
<tr>
<td>management software</td>
<td>from CRM to third-party communication management software.</td>
<td></td>
</tr>
<tr>
<td>Data between CRM system and BW system</td>
<td>Evaluation of interactive scripting using BW</td>
<td>Manual synchronization of evaluation data from CRM to BW</td>
</tr>
</tbody>
</table>

### Network and Communication Security

#### Communication Channel Security

#### Communication Channels Used in IC WinClient

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication between CRM and ERP</td>
<td>Action box communicates with ERP system via RFC</td>
<td>Business partner data, ERP sales order number, CRM activity number depending on BOR objects specified</td>
<td>(Optional) This communication channel is used when IC agents call certain action box transactions.</td>
</tr>
<tr>
<td>Communication between CRM system and third-party telephony switch</td>
<td>SAPphone API communicates with third-party telephony switch via RFC</td>
<td>Incoming call data is exchanged</td>
<td>(Optional) This communication channel is used when IC agents handle telephone calls through SAPphone</td>
</tr>
<tr>
<td>Communication between broadcast messaging client and CRM Server</td>
<td>HTTP</td>
<td>Text messages</td>
<td>(Optional) This communication channel is used when IC supervisors need to send text messages to IC agents</td>
</tr>
</tbody>
</table>

For information on how to secure communication channels, see the SAP NetWeaver security guide.

### Network Security

#### IC WinClient

The IC WinClient is an application on the CRM Server. For information on network security, see CRM Server [Seite 215].
Broadcast Messaging

Broadcast messages are normally sent from the CRM Server to the front end via HTTP protocol. If a secure connection is needed, broadcast messaging can be configured to use HTTPS protocol. For more information, see the Implementation Guide for Interaction Center WinClient → Visible Components → Define Broadcast Messaging Profiles.

Communication Destinations

Connection Destinations for IC WinClient

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to ITS</td>
<td>No</td>
<td>HTTP</td>
<td></td>
<td>Access remote ERP system using ITS. This communication can be secured by HTTPS. For details, see the SAP NetWeaver security guide.</td>
</tr>
<tr>
<td>Connection to remote ERP or CRM</td>
<td>No</td>
<td>RFC</td>
<td>Communication user or individual user</td>
<td>Access remote ERP system or CRM system using RFC. You could secure RFC over Secure Communication Network. For details, see the SAP NetWeaver security guide.</td>
</tr>
</tbody>
</table>

Data Storage Security

Data Processed in IC WinClient

<table>
<thead>
<tr>
<th>Data</th>
<th>Where Stored</th>
<th>When Stored</th>
<th>Type of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing data</td>
<td>CRM system</td>
<td>Post installation</td>
<td>Read/change/delete/create</td>
</tr>
<tr>
<td>Application data</td>
<td>CRM system</td>
<td>User request</td>
<td>Read/change/create</td>
</tr>
<tr>
<td>Application data</td>
<td>BW system</td>
<td>Interactive scripting evaluation</td>
<td>Change</td>
</tr>
</tbody>
</table>

Customizing data can be changed only by persons with CRM customizing authorization. This is normally done by the system administrator during system installation. CRM application data is protected at individual level. Depending on the role of the IC agent assigned, he/she could access, create, or change application data, for example, create a service order, update business partner data.

Security for Additional Applications

The IC WinClient uses the following dependent applications:

- SAPconnect
  Internal application from SAP Basis.
SAPconnect connects to an external server to provide e-mail functionality. It may be subject to e-mail spam and virus attack. We recommend setting up an external e-mail server with e-mail spam and e-mail virus cleaning.

- External Exchange Server
  Third-party application for e-mail. We recommend setting up e-mail spam and e-mail virus cleaning.

- HR (internal)
  SAP internal application for building a human resources structure. The IC WinClient HR is based on the HR structure from SAP HR. In the IC WinClient, the HR module is used to assign different system privileges to different users. An IC profile, which defines the UI layout and accessible functions, is assigned to an organizational unit. Any user belonging to this organizational unit can access only the functions assigned in this profile.

Other Security-Relevant Information

JavaScript is used extensively in the IC WinClient, for example, in the business partner search and universal inbox.

Trace and Log Files

The following trace and log files are provided by the IC WinClient:

- CRM related activities such as user logon and user logoff are logged in a report in the CRM system.

- E-mail using SAPconnect is traced on the CRM Server.

Appendix

Checklists

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td>Each e-mail address must be defined as a recipient to receive e-mail.</td>
<td>In transaction SO28, verify that the address is maintained.</td>
</tr>
<tr>
<td>Broadcast messaging</td>
<td>Where required, check that an HTTPS connection is configured for broadcast messaging profiles.</td>
<td>If you want broadcast messaging to use a secure HTTPS connection, the HTTPS Connection field must be selected for the broadcast messaging profile in Customizing for Interaction Center WinClient → Visible Components → Define Broadcast Messaging Profiles.</td>
</tr>
</tbody>
</table>
Interaction Center WebClient

Introduction

Interaction Center WebClient [Extern] (application component CRM-IC)

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most Relevant Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server</td>
<td>SAP Web Application Server security guide</td>
<td></td>
</tr>
<tr>
<td>Business Communication Broker (BCB)</td>
<td>SAP NetWeaver security guide</td>
<td>SAP NetWeaver Connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>security guide</td>
</tr>
<tr>
<td>Software Agent Framework</td>
<td>SAP Customer Relationship Management (CRM)</td>
<td>Software Agent Framework</td>
</tr>
<tr>
<td></td>
<td>security guide</td>
<td>[Seite 221]</td>
</tr>
<tr>
<td>Interaction Center Manager</td>
<td>SAP Customer Relationship Management (CRM)</td>
<td>Interaction Center Manager</td>
</tr>
<tr>
<td></td>
<td>security guide</td>
<td>[Seite 179]</td>
</tr>
<tr>
<td>Interaction Center WinClient</td>
<td>SAP Customer Relationship Management (CRM)</td>
<td>Interaction Center WinClient</td>
</tr>
<tr>
<td></td>
<td>security guide</td>
<td>[Seite 157]</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

Security is necessary because:

- The IC WebClient synchronizes contact attached data from communication management software. It is important to protect this data from unauthorized use because this data could include personal data or restricted business data such as contract order data.
- Interaction center agents can log on to the CRM system and access CRM data such as customer contract data and customer master data. It is crucial to protect customer-sensitive data.

Important SAP Notes

⚠️ Check regularly which SAP Notes are available about the security of the application.

Important SAP Notes

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>844929</td>
<td>Using the IC WebClient in Extranet/Internet</td>
<td></td>
</tr>
</tbody>
</table>
Technical System Landscape

Technical System Landscape of Interaction Center WebClient

Key

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICI</td>
<td>Integrated Communication Interface</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Relational Database Management System</td>
</tr>
<tr>
<td>APO</td>
<td>Advanced Planning and Optimization</td>
</tr>
<tr>
<td>BW</td>
<td>SAP Business Information Warehouse</td>
</tr>
<tr>
<td>OLTP</td>
<td>Online Transaction Processing System</td>
</tr>
</tbody>
</table>

User Administration and Authentication

User Management

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User maintenance (transaction SU01)</td>
<td>See: [User Management and Authentication][1] [User Management][2]</td>
</tr>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>You use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
</tr>
<tr>
<td>User Management Engine (UME)</td>
<td>This is mainly for defining users in running the IC WebClient in the SAP Enterprise Portal.</td>
</tr>
</tbody>
</table>

No user is delivered. You need to create the following users:

- RFC user to connect to back-end ERP system
This user is optional. You can create it to execute functions in the ERP system from the transaction launcher if you do not want to use the current logon user to connect to back-end ERP users. 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 kind of user is employed, be sure to provide appropriate authorization, neither insufficient nor overpowered.

- Individual users

Users on CRM Server who can access all functionalities in IC WebClient scenarios

Standard tools are employed for user administration.

**User**

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>Created by CRM system administrator for accessing IC WebClient application</td>
</tr>
<tr>
<td>CRM system</td>
<td>Customizing user</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>Created by CRM system administrator for customizing IC WebClient</td>
</tr>
<tr>
<td>ERP back end</td>
<td>End user</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>(Optional) Created by administrator of ERP back end. This user is employed if you want to use the transaction launcher to access functions from ERP. (User for launch transaction generation depends on RFC destination – either specific user or RFC user.)</td>
</tr>
<tr>
<td>ERP</td>
<td>End user</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>(Optional) Created by administrator of ERP system. This user is for</td>
</tr>
</tbody>
</table>
accessing ERP data through employee interaction center.

**User Data Synchronization**

If the employee interaction center is used, employee data from ERP is replicated to business partner data in CRM and vice versa.

If predictive dialing is used, call list data is synchronized between the CRM system and third-party communication management software by the IC manager.

**Authorizations**

The IC WebClient uses the CRM standard for authorizations.

No roles are delivered with this application. However, one CRM back-end role (SAP_PCC_IC_AGENT) is delivered with SAP Enterprise Portal (SAP EP). If you run this application in SAP EP, the CRM back-end user has to be assigned to this CRM back-end role.

**ABAP Stack Standard Roles Used by mySAP CRM**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_PCC_IC_AGENT</td>
<td>SU01 IC agent user</td>
</tr>
</tbody>
</table>

If SAP EP is used to access IC functions, it is very important to match roles between SAP EP and the CRM Server. For more information, see Authorizations [Seite 37].

**Standard Authorization Objects**

The following table shows the security-relevant authorization objects used in the IC agent scenario.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_TABU_DIS</td>
<td>ACTVT</td>
<td>02, 03</td>
<td>CRMC or CRMS</td>
</tr>
<tr>
<td></td>
<td>DICBELCLS</td>
<td></td>
<td>For all IC Customizing</td>
</tr>
<tr>
<td>BSP_APPL</td>
<td>BSP_APPL</td>
<td></td>
<td>This authorization is</td>
</tr>
</tbody>
</table>
Network and Communication Security

Communication Channel Security

Communication Channels Used in IC WebClient

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication between Web browser and SAP Web AS</td>
<td>HTTP/HTTPS</td>
<td>User requests are transferred between Web browser and SAP Web AS. Login information and</td>
<td>Used when IC agents log into CRM Server from Web browser. User sensitive data must be protected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>subsequent requests from browser are transferred from browser to SAP Web AS.</td>
<td>To configure SSL over SAP Web AS, see SAP NetWeaver security guide.</td>
</tr>
<tr>
<td>Communication channel between</td>
<td>HTTP/HTTPS</td>
<td>Each IC WebClient application session</td>
<td>Used when IC WebClient is initiated.</td>
</tr>
</tbody>
</table>

For protecting a People-Centric UI application. For a user to access a People-Centric UI application through the transaction launcher, the user must have authorization to access the People-Centric UI application. For more information, see People-Centric User Interface [Seite 226].

(Optional) This authorization object is used in the auto suggest in the IC WebClient. For more information, go to SAP Help Portal and choose Documentation ® mySAP Business Suite ® mySAP Customer Relationship Management ® SAP CRM 5.0 ® Components and Functions ® Basic Functions ® Multilevel Categorization ® Authorizations for the Category Modeler.
### Communication Between Components Residing in Different ABAP Sessions of IC WebClient

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Components residing in different ABAP sessions of IC WebClient</td>
<td>Consists of multiple ABAP sessions running concurrently.</td>
<td>To enable HTTPS, an additional HTTP destination is created (see Communication Destinations below).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure SSL over SAP Web AS, see SAP NetWeaver security guide.</td>
</tr>
</tbody>
</table>

### Communication Between Remote CRM System or Remote ERP System

- **HTTP through SAP Internet Transaction Server (ITS):** ITS connects to the remote CRM system or ERP system through RFC.
- **Business transactions and business objects are exchanged between ERP and CRM.**
- *(Optional)* Used when IC agent in CRM tries to access data in ERP system or remote CRM system through launch transaction.

### Communication Between Same CRM System

- **HTTP through People-Centric UI**
- *(Optional)* Used when IC agent tries to launch a People-Centric UI application on the same CRM server through launch transaction.
- Configure HTTP over SSL in SAP Web AS.

### Communication Between CRM System and Communication Management Software Such as Telephony, E-Mail Router

- **Business Communication Broker (BCB) API** communicates with communication management software via SOAP.
- **Data (such as incoming call, contact attached data, e-mail) is transferred from communication management software to CRM system.**
- Used whenever multichannel is employed in IC WebClient to handle telephone calls, e-mails, chat, and so on.

### Communication Between CRM System and Third-Party Telephony Switch

- **SAPphone API** communicates with third-party telephony switch via RFC.
- **Incoming call data is exchanged.**
- *(Optional)* Used when IC agents handle telephone calls through SAPphone.

### Communication Between CRM and TREX

- **SOAP through TREX API**
- *(Optional)* Used when IC agents require the knowledge search through TREX search engine. For more information, see Knowledge Search on SAP Help Portal under mySAP Customer Relationship Management.

---

To start the IC in a secure environment, use default_https.htm to start the application. Subsequent HTTP calls automatically use secure HTTP call. An additional RFC communication needs to ensure the subsequent call is HTTPS. See the **Connection Destinations** table below.
Network Security

If there is a firewall between agents' machines and the CRM Server, and if agents access the IC WebClient from another network or from the Internet by launching the interaction center BSP URL, the Business Server Page (BSP) ports for HTTP/HTTPS have to be opened in the firewall.

Communication Destinations

You have to create the following destinations:

Connection Destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TREX server</td>
<td>No</td>
<td>HTTP</td>
<td></td>
<td>(Optional) Part of configuration of TREX</td>
</tr>
<tr>
<td>Remote CRM</td>
<td>No</td>
<td>RFC</td>
<td></td>
<td>(Optional) Communication to remote ERP or remote CRM through transaction launcher</td>
</tr>
<tr>
<td>ERP</td>
<td>No</td>
<td>RFC</td>
<td></td>
<td>(Optional) Communication to remote ERP through transaction launcher. This is out of scope of IC WebClient. It is part of Business Object Repository (BOR) setup.</td>
</tr>
<tr>
<td>ERP</td>
<td>No</td>
<td>RFC</td>
<td></td>
<td>(Optional) Communication to ERP to retrieve employee data if you are using employee interaction center.</td>
</tr>
<tr>
<td>Third-party telephony server</td>
<td>No</td>
<td>RFC</td>
<td></td>
<td>(Optional) Only if IC agents handle calls using SAPphone. For more information, see SAPphone on SAP Help Portal under SAP NetWeaver.</td>
</tr>
</tbody>
</table>

An additional communication destination is added for HTTPS.
### Data Storage Security

#### Stored Data

<table>
<thead>
<tr>
<th>Data</th>
<th>Where Stored</th>
<th>When Stored</th>
<th>Type of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customization</td>
<td>SAP Web AS database</td>
<td>Post installation</td>
<td>Read/write/change/delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Only by user with CRM customization authorization</td>
</tr>
<tr>
<td>Application data</td>
<td>SAP Web AS database</td>
<td>IC user logon/request</td>
<td>Read/write/change/delete</td>
</tr>
<tr>
<td>Generated class</td>
<td>SAP system</td>
<td>During customizing of transaction launcher</td>
<td>Read/write/change/delete</td>
</tr>
<tr>
<td>Configuration</td>
<td>SAP system</td>
<td>Post installation</td>
<td>Read/write/change</td>
</tr>
</tbody>
</table>

The IC WebClient supports/requires a Web browser as the 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 persons with a CRM Customizing authorization. This data is normally 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 Simple 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 very sensitive data and is not accessible from outside the current Web AS, so there is no severe security risk. This information is removed from the server side cookie if and when the application session has shut down correctly.

### Security for Additional Applications

The following additional applications are associated with the IC WebClient or delivered with it:

- Third-party communication management software
  - Has its own authentication and authorization mechanism to ensure security. Does not presently support HTTPS communication.

- Business Communication Broker (BCB)

- SAPphone
  - Provides a telephony function for the IC.
There are no particular front-end clients that deviate from the standard SAP system.

Additional Applications

<table>
<thead>
<tr>
<th>Additional Application</th>
<th>Vendor</th>
<th>Security Guide</th>
<th>Special Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS</td>
<td>SAP internal</td>
<td>SAP NetWeaver Security Guide</td>
<td>No</td>
</tr>
<tr>
<td>People-Centric UI</td>
<td>SAP internal</td>
<td>SAP CRM Security Guide: People-Centric User Interface [Seite 226]</td>
<td>To use a People-Centric UI based application within the IC WebClient, users must have authorization to start the People-Centric UI based application.</td>
</tr>
<tr>
<td>BCB</td>
<td>SAP internal</td>
<td>SAP NetWeaver Security Guide</td>
<td>No</td>
</tr>
<tr>
<td>SAPphone</td>
<td>SAP internal</td>
<td>SAP NetWeaver Security Guide</td>
<td>No</td>
</tr>
</tbody>
</table>

Other Security-Relevant Information

Active Code

<table>
<thead>
<tr>
<th>Active Code</th>
<th>Location</th>
<th>Functions Disabled Without This Active Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java applet</td>
<td>Free seating</td>
<td>Free seating is an IC capability that allows agents to utilize communication services provided at different workplaces.</td>
</tr>
<tr>
<td>Java applet</td>
<td>IC notify</td>
<td>Polling messages from ABAP session to Web browser. (alerts, multichannel management) use this applet.</td>
</tr>
<tr>
<td>JavaScript</td>
<td>Widely used in front end</td>
<td>IC WebClient</td>
</tr>
</tbody>
</table>

Two Java applets are used in the IC agent application. Because these two applets are not digitally signed, we recommend running them in the intranet.

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 Web AS cache:

- Messages exchanged between communication management software and CRM Server
- Messages exchanged between ABAP sessions

Trace by default is turned off. To turn on the trace and change the trace level, see Administration of the Internet Communication Manager [Extern] on SAP Help Portal under SAP NetWeaver.

Appendix

Checklists

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS communication between different ABAP sessions</td>
<td>SAPCRYlib is installed and client certificate is properly imported</td>
<td>In transaction SM59, choose the RFC destination for connecting two IC WebClient sessions, and choose <em>Connection Test</em>.</td>
</tr>
</tbody>
</table>
**E-Mail Response Management System**

**Introduction**

**E-Mail Response Management System [Extern]** (application component CRM-IC-EMS)

The E-Mail Response Management System (ERMS) is based on SAP Web Application Server (SAP Web AS) 6.40 and CRM 5.0. ERMS runtime runs on top of the workflow system. The design time uses the People-Centric UI framework.

**Related Security Guides**

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most Relevant Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server</td>
<td>SAP Web Application Server security guide</td>
<td></td>
</tr>
<tr>
<td>People-Centric UI</td>
<td>SAP Customer Relationship Management (CRM) security guide</td>
<td>People-Centric User Interface [Seite 226]</td>
</tr>
<tr>
<td>Workflow</td>
<td>SAP Web Application Server security guide</td>
<td></td>
</tr>
</tbody>
</table>

**Why Is Security Necessary?**

The ERMS deals primarily with e-mail. Because of the openness of this communication channel (anybody can send an e-mail to this system), it is important to take necessary measures to:

- Ensure high availability of the system (that is, make sure the system is not brought down by massive numbers of requests)
- Protect the system from malicious e-mails containing viruses
- Protect data that is important in this application (such as personal information within the CRM system)

**Important SAP Notes**

⚠️ Check regularly which SAP Notes are available about the security of the application.
Technical System Landscape

ERMS Architecture

The entry point to ERMS runtime is SAPconnect [Extern]. 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 transaction SO28.

Once the workflow is started, it invokes the ERMS service manager which is the core of the ERMS runtime.

User Administration and Authentication

User Management

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User maintenance (transaction SU01)</td>
<td></td>
</tr>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>You use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
</tr>
</tbody>
</table>

No user is delivered. You need to create the following users:
- WF-BATCH
  User for the workflow system to be able to execute

- Individual users
  In addition to the above workflow user, it is necessary to:
  - Give the system administrator access to the modeling tools available for the ERMS
  - Create users for IC agents so that they can access the system and process incoming e-mails

### User

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Enterprise Portal</td>
<td>IC manager</td>
<td>No</td>
<td>Portal user with IC manager role</td>
<td>No</td>
<td>For using tools such as rule modeler, category modeler, and ERMS reports</td>
</tr>
<tr>
<td>CRM system</td>
<td>IC agent</td>
<td>No</td>
<td>Dialog</td>
<td>INIT</td>
<td>Created by CRM system administrator to allow agents to respond to e-mails</td>
</tr>
<tr>
<td>SAP Business Information Warehouse</td>
<td>ERMS administrator or IC manager</td>
<td>No</td>
<td>Dialog</td>
<td>No</td>
<td>For access to ERMS reports in SAP BW</td>
</tr>
</tbody>
</table>

The user with a default password is required to log into the system to change the default password.

### User Data Synchronization

Reporting data is stored initially in CRM. For historic reporting, it must be transferred to the BW system.

### Integration Into Single Sign-On Environments

Single sign-on is supported if the ERMS tools are run in SAP Enterprise Portal.

### Authorizations

The ERMS uses the CRM standard for authorizations.

To enable ERMS administrators to use the ERMS design time tools (transaction PFCG), you must assign ERMS administrators to CRM role SAP_PCC_ERMS_ADMIN. This role includes the necessary authorization to access:

- 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 E-Mail Response Management System → Define Repository. Select context ERMS and double-click Authorization Groups. Finally, add authorization CRM_ERMS_P to role SAP_PCC_ERMS_ADMIN, and set the following parameters accordingly:

- Activity
- ERMS Authorization Group
- Context

Network and Communication Security

Communication Channel Security

The preferred way to configure your system is to have a general purpose e-mail server such as Microsoft Exchange, then have filtering tools for spam and viruses, and at the end, hand over the e-mail to CRM ERMS for processing.

Because SAPconnect uses SMTP for receiving e-mails, another (but not recommended) way to configure your system is to send an e-mail directly to the CRM system and have it processed by the ERMS. For information about SAPconnect, see SAP Note 738326.

Data Storage Security

ERMS data is stored in the CRM database like any other CRM information. It is not necessary to add security. The stored data can be classified as follows.

### Stored Data

<table>
<thead>
<tr>
<th>Data</th>
<th>Where Stored</th>
<th>When Stored</th>
<th>Type of Access</th>
<th>Who Can Access It</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail document</td>
<td>CRM system → Business Workplace persistence</td>
<td>When e-mail arrives</td>
<td>Read/delete</td>
<td>ERMS routes the e-mail to an organizational unit. Users in that organization can access the e-mail document.</td>
</tr>
<tr>
<td></td>
<td>Also database table CRMD_ERMS_CNTNT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERMS fact base</td>
<td>CRM system → Workflow container</td>
<td>When ERMS processes an e-mail</td>
<td>Read/write/delete/change</td>
<td>ERMS, ERMS administrator in ERMS log, or transaction SWI1 (only in read mode)</td>
</tr>
<tr>
<td>ERMS rules</td>
<td>CRM system → ERMS repository (customizing data)</td>
<td>When rules are maintained</td>
<td>Read/write/delete/change</td>
<td>ERMS administrator</td>
</tr>
<tr>
<td>ERMS configuration</td>
<td>CRM system → ERMS repository</td>
<td>During configuration</td>
<td>Read/write/delete/change</td>
<td>ERMS administrator</td>
</tr>
</tbody>
</table>
Trace and Log Files

Log information is available through transaction CRM_ERMS_LOGGING. The log provides the following information:

- Services invoked by ERMS service manager
- Data gathered by ERMS services
- Rules evaluated
- Categories assigned
- Execution times for different services

Appendix

Checklists

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict access to e-mail processing</td>
<td>Workflow e-mail task can be processed only by authorized organizational units and/or users.</td>
<td>In the SAP menu, choose Interaction Center → E-Mail Response Management System → Settings → Assign Agent for E-Mail Handling. Click 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.)</td>
</tr>
<tr>
<td>Restrict access to e-mail processing</td>
<td>Authorized agents are properly assigned to the organizational unit.</td>
<td>For the e-mail workflow task above, go to the SAP menu and choose Interaction Center → Supporting Processes → IC Structure → Change Organization and Staffing.</td>
</tr>
<tr>
<td>Restrict/allow access to certain policies in ERMS rule modeler</td>
<td>Use ERMS authorization group concept.</td>
<td>To define your authorization groups, use transaction CRMC_ERMS_REPOSITORY</td>
</tr>
</tbody>
</table>
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.
Interaction Center Manager

Introduction

The Interaction Center (IC) manager runs in SAP Enterprise Portal. The IC manager includes the following components:

- (People-Centric UI based) Call List Execution and Maintenance (application component CRM-IC-CAL)
- Manager Dashboard (application component CRM-IC-MDB)
- IC analytics, including interaction statistics and interactive scripting (application component CRM-ANA-IC)

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most Relevant Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server</td>
<td><a href="Extern">SAP Web Application Server Security Guide</a></td>
<td></td>
</tr>
<tr>
<td>SAP Enterprise Portal 6.0</td>
<td><a href="Extern">SAP Enterprise Portal 6.0 Security Guide</a></td>
<td></td>
</tr>
<tr>
<td>People-Centric UI</td>
<td><a href="Extern">SAP Customer Relationship Management (CRM) Security Guide</a></td>
<td>People-Centric User Interface [Seite 226]</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

Security is necessary to prevent attacks from the Internet and to protect data. Because the IC manager can access the CRM system via the browser even if the IC manager does not have a user in CRM, it is very important to define the authority of the IC manager with regard to system access. For example, you should consider whether to allow an IC manager to delete a program after logging on to a back-end CRM system via the browser.

The IC manager can perform functions such as monitoring each agent’s call status, designing scripts to guide 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 stolen.

User Administration and Authentication

User Management

The IC manager employs standard user management tools to maintain users. See the following table:

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Maintenance (transaction SU01)</td>
<td></td>
</tr>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>You use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
</tr>
<tr>
<td>User Management Engine (UME)</td>
<td>Mainly for defining users in running the IC Manager in the SAP Enterprise Portal.</td>
</tr>
</tbody>
</table>

No standard users are delivered. You need to create the following users:
• CRM user
  If users want to access IC Manager functions, we recommend your system administrator to create users and assign them to role SAP_PCC_IC_MANAGER (see also Authorizations). All functions for the IC Manager are defined in this role.

• Portal user
  The portal role is embedded in the IC Manager business package which you can download from iViewStudio.

A portal may have several back-end systems such as CRM, BW. The portal user is mapped to the back-end CRM or BW system, but the back-end users are invisible to the portal users. Users in CRM can access all functionality on the People-Centric UI of Call List Management / Dashboard.

User

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Enterprise Portal</td>
<td>End user</td>
<td>No</td>
<td>Dialog</td>
<td></td>
<td>Created by portal administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog</td>
<td></td>
<td>Created by CRM system administrator</td>
</tr>
<tr>
<td>BW system</td>
<td>End user</td>
<td>No</td>
<td>Dialog</td>
<td></td>
<td>Created by BW system administrator</td>
</tr>
</tbody>
</table>

The default password for the CRM system and BW system is necessary when creating a new user in those systems. When the user logs on to the system, he or she is required to change the password. 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 CRM system. There is no user data synchronization.

Integration Into Single Sign-On Environments
The application accepts SAP logon tickets.
The application does not accept X.509 digital certificates.

When the CRM user or BW user is integrated into SAP Enterprise Portal, it is SSO enabled.

Authorizations
The IC Manager uses the CRM standard for authorizations.

No roles are delivered with this application. However, one back-end role (SAP_PCC_IC_MANAGER) is delivered with the CRM back end. This role corresponds to the IC manager role, which is delivered with several versions of the CRM business package. If you run this application in SAP Enterprise Portal, you assign your users to these roles.

The following table shows the security-relevant authorization objects used in the IC agent scenario.

Standard Authorization Objects
<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSP_APPL</td>
<td>BSP_APPL</td>
<td>SPACE</td>
<td>This authorization is for protecting the People-Centric UI application. This authorization object is included in the SAP_PCC_IC_MANAGER roles for different People-Centric UI applications that can be accessed by the IC Manager.</td>
</tr>
<tr>
<td></td>
<td>BSP_VIEW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRM_IC_MDB</td>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
<td>This authorization object is used in IC manager dashboard in SAP Enterprise Portal.</td>
</tr>
<tr>
<td>CRM_BM</td>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
<td>Only users with this authorization in their user profile can start the broadcast messaging server application for IC manager.</td>
</tr>
<tr>
<td>S_RFC</td>
<td>ACTVT</td>
<td>16</td>
<td>This authorization object is used in the interactive scripting editor to access two function groups:</td>
</tr>
<tr>
<td></td>
<td>RFC_NAME</td>
<td>CRM_IC_SCRIPTING_PERSIST</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RFC_TYPE</td>
<td>CRM_IC_XML_STORAGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FUGR</td>
<td></td>
</tr>
<tr>
<td>CRM_IC_SCR</td>
<td>ACTVT</td>
<td>02 03 06</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SCR_GRP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Network and Communication Security**

**Communication Channel Security**

Because the IC manager application runs in the Web browser, it needs to communicate with the back-end CRM Server. An HTTP(S) communication channel is required.

**Broadcast Messaging Service**

- HTTP(S) communication from browser to CRM Server
- HTTP(S) communication between CRM Servers for sending messages to agents

**Manager Dashboard**
• HTTP(S) communication from browser to CRM Server
• Communication between CRM Server and communication management software via SOAP


**Data Storage Security**

No temporary data is stored.

The application supports/requires a Web browser as the UI.

Broadcast messaging uses cookies to store some UI favorites on the client side. This data stays there unless it is manually deleted. No sensitive data is stored in the cookie so no particular measures to protect the cookie are required.

Dashboard stores personalization data (for example, application layout) on the client side. This data does not require further security protection.

**Security for Additional Applications**

There are no settings in other applications within the system landscape that are important for the security of this application.

**Additional Applications**

<table>
<thead>
<tr>
<th>Additional Application</th>
<th>Vendor</th>
<th>Security Guide</th>
<th>Special Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>People-Centric UI</td>
<td>SAP internal</td>
<td>SAP Customer Relationship Management (CRM) Security Guide → People-Centric User Interface [Seite 226]</td>
<td>To use a People-Centric UI based application within the IC manager, users must have authorization to start the People-Centric UI based application.</td>
</tr>
</tbody>
</table>

**Other Security-Relevant Information**

If your security policy does not allow the use of active code, you cannot use dashboard.

⚠️

Generally speaking, using active code such as applets and ActiveX controls poses a security risk.

**Active Code**

<table>
<thead>
<tr>
<th>Application</th>
<th>Active Code</th>
<th>Functions Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive scripting editor</td>
<td>Java plug-in</td>
<td>Interactive scripting editor cannot be started</td>
</tr>
</tbody>
</table>

**Trace and Log Files**

The SAP Enterprise Portal standard is used for tracing and logging at system level and application level.

**Appendix**

**Checklists**
<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast messaging service for supervisors</td>
<td>For authorization object CRM_BM, check that field ACTVT has value 16</td>
<td>In role maintenance (transaction PFCG), enter role SAP_PCC_IC_MANAGER or any role used to create supervisors, and choose Display Role. On the Authorizations tab page, choose Display Authorization Data. In the Utilities menu, choose Technical Names On (if not on already).</td>
</tr>
<tr>
<td>Interactive scripting editor</td>
<td>For authorization object S_RFC, check that: Field ACTVT has value 16 Field RFC_NAME has value CRM_IC_SCRIPTING_PERSIST or CRM_IC_XML_STORAGE Field RFC_TYPE has value FUGR</td>
<td>As above</td>
</tr>
<tr>
<td>Interactive scripting editor</td>
<td>For authorization object CRM_IC_SCR, check that: Field ACTVT has value 02, 03, or 06 Field SCR_GRP has value &lt;blank&gt;</td>
<td>As above</td>
</tr>
</tbody>
</table>
Interaction Center: Workforce Management Services

Introduction

This topic describes the security measures for the following two services of Interaction Center Workforce Management:

- Interaction Center (IC) Agent Scheduling
- Multisite Workforce Deployment

The components of Multisite Workforce Deployment and IC Agent Scheduling run on the Java 2 Enterprise Edition (J2EE) Engine and can be accessed through the SAP Enterprise Portal.

Why Is Security Necessary?

IC Agent Scheduling and Multisite Workforce Deployment services use the J2EE Engine services, such as, JCO, Logging, and HTTP. Security measures are necessary to prevent unauthorized access and entry to any component or service, for example, in the following scenarios:

- A user who has unauthorized entry into the Visual Administrator can easily stop the Workforce Management Services component.
- A user with access to the IC Agent Scheduling - Web Administrator Tool can misuse rights and stop the calculation services by setting the number of available solvers to 0.
- A Denial of Service (DOS) attack while deploying the components of Workforce Management. This attack involves overloading the components with unnecessary and irrelevant HTTP requests. This leaves little processing time for relevant requests. To combat such security threats, the J2EE Server must deploy strict security measures.
- Network and communications are compromised. Most of the communication between Workforce Management Services is done using HTTP protocols.

User Administration and Authentication

User Management

Listed in the table below are the tools and functions used to manage users:

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal AdminCenter for the following two roles: User Portal Administrator</td>
<td>Portal user administration</td>
<td>SAP Enterprise Portal must be running.</td>
</tr>
<tr>
<td>SU01 - SAP NetWeaver transaction</td>
<td>SAP NetWeaver user administration</td>
<td>SAP NetWeaver must be running.</td>
</tr>
<tr>
<td>PCFG - SAP NetWeaver</td>
<td>SAP NetWeaver role</td>
<td>SAP NetWeaver must be running.</td>
</tr>
</tbody>
</table>
For each Calculation Server running the Calculation Services, a system user must be configured. Unlike portal administration, this configuration refers to a backend system user (user needed by the application to function). This user is needed by the component when accessing its own data stored in the SAP NetWeaver system and for interaction with client applications submitting calculation requests.

This user has to be created after the deployment of the Multisite Workforce Deployment or IC Agent Scheduling on each Calculation Server.

**User Types**

- **Portal user:**
  
  You maintain this user in the Portal Admin Center. It is needed for accessing the Web Administration Tool in order to be able to administer and supervise the Calculation Services.

- **Backend system user:**
  
  You maintain this user in the Workforce Management Calculation Services. On the Extended Configuration Manager (XCM) page, enter an SAP NetWeaver system with a user name and password. This is for the application to access the SAP NetWeaver system for its data related tasks as well as for interaction with client applications submitting calculation requests. The XCM configuration has to be done on each Calculation Server for which the Calculation Services has been deployed. It is expected that XCM will provide configuration copying between Calculation Servers.

  For more information about calculation services, see Workforce Management Services on Help Portal.

**Integration Into Single Sign-On Environments**

Multisite Workforce Deployment and IC Agent Scheduling support Single Sign-On through the SAP Enterprise Portal. It accepts logon tickets and X.509 digital certificates.

**Authorizations**

These two services can be accessed through the SAP Enterprise Portal. They use two roles:

- **User**
This is a role of a regular portal user, who accesses the business functionality of the application. This role is mapped to a regular SAP NetWeaver user (dialog type).

- **Portal Administrator**
  A role that is meant to access the administrative part of the application. This role is also mapped to a regular SAP NetWeaver user of dialog type.

The portal administrator must be given access to the portal iView containing the Multisite Workforce Deployment - Web Administration Tool.

### Network and Communication Security

#### Communication Channel Security

Multisite Workforce Deployment and IC Agent Scheduling use the following communication channels:

- **RFC or SAP Java Connector (JCo) to connect to SAP NetWeaver**
  This is mainly used for transferring application data.

- **HTTP or HTTPS for User Interaction and Inter-Calculation Server node Communication**
  Again, this is mainly used to issue commands and transfer application data.

  Inter-Calculation Server node communication is done only in the case of the deployment of Calculation Services on multiple machines. One of the Calculation Servers is also used to run the Web Administration Tool. Therefore, direct user access must only be provided to the Calculation Server that is running the Web Administration Tool. As an additional security measure, the other machines running the Calculation Services components must be protected by a firewall. The network setup must protect the HTTP communication between these machines.

#### Network Security

These functions also use HTTP/HTTPS, since they are:

- Configured for the J2EE Engine
- Used to access the SAP NetWeaver system for data access

From a security point of view, these are the components of interest:

- Calculation Service-J2EE: Web Administration Tool, Request Manager, Solver
- Calculation Service-CRM/R3: package WFD_CALCSERVICES.

Only Web Administration Tool is a public component all others are internal and must be protected against direct user access, possibly by a firewall blocking http access.

Depending on the available resources and how the landscape is setup, these are the recommendations for security:

- when there is only https access from SAP portal to Web Administration Tool
all components can be deployed on server(s) behind a firewall blocking public http access and allowing https access. If the deployment is done on more than one server, intra-net http access must be allowed between the servers.

- when there is http access from SAP portal to WAT-UI
  Web Administration Tool deployed on a server where public http is allowed, all other components deployed on server(s) behind a firewall blocking public http access but allowing intra-net http access (including the server where Web Administration Tool is deployed).

In case public http access is allowed to servers running the internal components (all components except Web Administration Tool), the application is vulnerable to DOS (Denial of Access) attacks.

The J2EE components are packaged together in the same .ear file, so technically they are deployed together. However, using the Web Administration Tool, the internal components can be selectively enabled as to which is allowed to run on a which server. Please refer to the Web Administration Tool documentation for further details regarding Calculation Services configuration.

### Communication Destinations

The table below shows an overview of the communication destinations used by the components.

#### Connection Destinations

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM/R3</td>
<td>Yes</td>
<td>JCO/RFC</td>
<td>System user created through XCM</td>
<td>For more information, see Configure Calculation Servers of Workforce Management Services on Help Portal.</td>
</tr>
<tr>
<td>Calculation Server</td>
<td>Yes</td>
<td>HTTP/HTTPS</td>
<td>System user created through XCM / Portal User</td>
<td>For more information, see Configure Calculation Servers of Workforce Management Services on Help Portal.</td>
</tr>
</tbody>
</table>

### Data Storage Security

The application data is:

- Stored in SAP Netweaver and the application configuration data is stored in SAP Netweaver and XCM. The data is protected against unauthorized access through user name and password.
- Accessible through the web browser and SAP GUI. Persistent cookies are not used at any time.
Other Security-Relevant Information

Due to complex user interface requirements, both Multisite Workforce Deployment and IC Agent Scheduling use JavaScript in the web browser. Hence, JavaScript must be enabled in the web browser to provide proper functionality.

Trace and Log Files

These functions also use the standard J2EE Engine logging and tracing mechanism. Therefore, the access and protection of the log and trace files is managed by J2EE Engine.

Checklist

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Administration Tool</td>
<td>Portal Admin log-on</td>
<td>Log on as portal administrator and access the Workforce Management Calculation Services. Log on as regular portal user and access to the Workforce Management Calculation Services should be disabled.</td>
</tr>
</tbody>
</table>
# Channel Management

## User Administration and Authentication

The type of the user administration differs depending on the use of Internet Sales CRM, R/3 or Enterprise Portal as explained in the following sections.

### User Management Tools when using ISA within Portal (Channel Management)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-Based User Management</td>
<td>For configuration documentation, see SAP Solution Manager.</td>
<td>Only applicable for B2B users with SU01 user type. As authentication value SU01 “user ID” must be used. Only for ISA for CRM.</td>
</tr>
<tr>
<td>LDAP update</td>
<td>Refer to the Portal Documentation and note 629442.</td>
<td>Only for EP 5.0 together with ISA for CRM</td>
</tr>
</tbody>
</table>

### User types for ISA for CRM and Channel Management

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM</td>
<td>Service (anonymous) user for stateless connection</td>
<td>No</td>
<td>SU01 service user</td>
<td>No</td>
<td>SU01 User for establishing the stateless connection between CRM and ISA.</td>
</tr>
<tr>
<td>CRM</td>
<td>ISA user</td>
<td>No</td>
<td>SU01 dialog user</td>
<td>No</td>
<td>The user that logs into ISA. The full state ISA connection is established with it.</td>
</tr>
<tr>
<td>CRM</td>
<td>ISA user</td>
<td>No</td>
<td>SU05</td>
<td>No</td>
<td>The user that logs into ISA.</td>
</tr>
</tbody>
</table>
Authorizations
The following table lists the roles that are created on the J2EE engine for each application when the application is installed.

### Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_INTERNET_CUSTOMER</td>
<td>SU01 ISA user in B2B shop and B2C shop (when the user is logged on).</td>
</tr>
<tr>
<td>SAP_CRM_ISA_UA_SUPERUSER</td>
<td>Refer to the Super User management documentation.</td>
</tr>
<tr>
<td>SAP_CRM_ISA_WEBSHOP_MANAGER</td>
<td>Refer to Shop Management and User Management documentation.</td>
</tr>
<tr>
<td>SAP_CRM_ISA_ITSLOGIN</td>
<td>Stateless user. For more information, refer to the Configuration Information of the Solution Manager.</td>
</tr>
</tbody>
</table>

The following new roles created for role-based authorizations are also valid for Channel Management.

### New Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2B_FULL</td>
<td>B2B with full document authorization</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2B_ORDER</td>
<td>B2B with full order and display sales order document authorization.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2B_VIEW</td>
<td>B2B with view only authorization</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_B2C</td>
<td>Full B2C authorization (when the user is logged on). This role will be assigned to a reference user.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_SHOPADMIN</td>
<td>Full shop management authorization.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_BOB_FULL</td>
<td>BOB with full sales order document and quotation authorizations.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_HOM_FULL</td>
<td>Hosted Order Management with full authorization.</td>
</tr>
<tr>
<td>SAP_CRM_ECO_ISA_WU_HOM_VIEW</td>
<td>Hosted Order Management with view only authorization.</td>
</tr>
</tbody>
</table>

Channel Management

In Channel Management, 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 Roles.

External Services Transaction are defined in SU22(type LS), for each BSP Application- View combination. We would deliver them for all Partner related applications. The default values would be set up according to Standard delivered Channel management scenario.
The Access Control Engine (ACE) is another important step towards Authorizations in Channel Management. This is a new tool developed to control access for external users. ACE is used in conjunction with ABAP Authorization concept to provide full security to the applications and data. For more information, refer to CRM Access Control Engine [Seite 238].

Delivered Roles for Channel Management:

- SAP_PCC_COL_PARTNEREMPLOYEE Channel Management – Partner Employee
- SAP_PCC_COL_PARTNERMANAGER Channel Management – Partner Manager
- SAP_PCC_COL_PARTNERMANAGER_CC Channel Management – Partner Manager Channel Commerce

Before mentioned CRM roles are also used for ISA in Channel Management.

Whether or not to use the standard delivered values. This would also depend on customizing. In case Customizing is changed, also the values for certain Authorization objects (which use customized values) should change.

Also if the scenario implementation at customer end, had new or enhanced features, this might also require enhancements to Authorizations.

With External Services transactions, the values delivered as 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 delivered values to the customer namespace and then change or maintain these values. This is also performed in transaction SU22. for details, refer to Note 449832(Maintenance of SU22 data).

**Transaction (Process) Types for Partner Roles controlled via Authorizations.**

In CRM 4.0 the transaction types used for partners were specified in a customizing table. These transaction types were the ones that partner was allowed to use.

From CRM 5.0 onwards we would use the standard mechanism of authorization checks for allowed transaction types for a given role/user.

The authorization objects for an user are: CRM_ORD_LP and CRM_ORD_PR. Please refer to the documentation of these objects in system to find the settings. Normally the allowed transaction types are set in object CRM_ORD_PR.

Note that the authorization given in first object overwrites the authorization allowed in second one.

Now you have to decide whether to adopt the delivered standard authorizations, which would be setup in the Channel Management roles, or to extend/adopt them to customer specific transaction types.

In case new transaction types are required for Channel Business, please create new roles and extend the authorizations for the above mentioned objects accordingly.

**Data Storage Security**

The data storage security is explained as follows:

**Channel Management**

In Channel Management, the data security is provided by ACE. The access to the data for the users is defined through a set of predefined rules in ACE. These set of rules are applied to the data when it is being created and stored and from this an ACL is generated. This ACL is then used during runtime to determine the extent of access the user has to the data.
Currently the ACE checks run only in CRM online for One Order objects. For products and Business Partner, they run only in Portal context.

The decision to activate or not to activate ACE lies on the fact, whether or not document level access check is required for the users. The Activation decision is now at three levels:

- System
- Users/User Groups
- Object Types

To get the ACE up and running, the customers must go through the Customizing under Customer Relationship Management → Basic Functions → Access Control Engine.

In addition, customers can define their own rules and access rights to provide additional access control based on their business requirements.

For Channel Management two ACE packages are delivered with pre-configured user groups and rights for different object types. These packages are:

- SAP_CRM_CHM_OO.
- SAP_CRM_CHM_ACCOUNT

For activation of these packages please use the transaction ‘ACE_ACTIVATION’. For further information on this please refer to the Implementation Guide under Customer Relationship Management → Basic Functions → Access Control Engine.

Please remember that there is no package delivered for Products, as the access to Products is restricted via the Catalog. As the checks are in place for portal access, customers are allowed to define their own rights and activate them to provide extra access control for the portal users.

Activation of these packages would ensure ACE security for Channel Management scenario.

**Security for outgoing content via e-mail (Adobe documents)**

In case of scenario where the Brand Owner is doing business with Partners who have no Portal access, e-mail communication would be used to pass over the CRM content.

There would be certain CRM documents (for e.g. Leads), which would be sent to partners for qualification. This communication would be over the e-mail and in Adobe format.

Apart from the Adobe document, the mail would also contain some attributes from the CRM documents itself.

If the content of the document being sent over the e-mail (insecure channel), is really sensitive. Then the customer should decide whether or not to use this functionality.
Channel Sales Management for High-Tech

Introduction
SAP Channel Sales Management for Hi-Tech is an ABAP based solution. It encapsulates the following functions which have been modeled as different applications:

- Design Registration (Based on Enterprise CRM Opportunities)
- Bill Up
- Channel Inventory Management
- Channel Inventory Reconciliation
- Inventory Reporting
- Resale Tracking & Claim Management
- Price Protection
- Sell-In (Sales to Channel Partner)
- Transmission Management

These applications enable processing of various channel sales related data, which also includes creation of sales documents in the CRM system and sales and invoicing documents in the back-end ERP system.

This chapter provides the security information for Channel Sales Management for Hi-Tech.

Why Is Security Necessary?
Security is necessary, because Channel Sales Management for Hi Tech:

- Accesses data in the CRM system, such as resale information, channel inventory information, price protection information, and other channel sales related information which is maintained in the CRM system
- Leads to creation of sales documents in the CRM system (which are replicated and invoiced in the backend ERP system)

Therefore, it is very important to restrict access to this data.

User Administration and Authentication
Channel Sales Management for Hi Tech uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology also apply to the Channel Sales Management for Hi Tech application.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to Channel Sales Management for Hi Tech in this topic.

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with Channel Sales Management for High Tech.

User Management
User management for Channel Sales Management for Hi Tech uses the mechanisms provided by the SAP Web Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for the application, see the sections below. In addition, we provide a list of the standard users required for operating Channel Sales Management for High Tech.
User Management Tools

<table>
<thead>
<tr>
<th>Tools</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Web AS ABAP (Transactions SU01, PFCG)</td>
<td>For more information, see Users and Roles (BC-SEC-USR).</td>
<td></td>
</tr>
</tbody>
</table>

User Types

The following users must be created for the Channel Sales Management for Hi Tech:

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory. User who can access channel sales transactions. Created by CRM system administrator.</td>
</tr>
<tr>
<td>CRM system</td>
<td></td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory. User who can process background jobs</td>
</tr>
<tr>
<td>ERP backend</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory. User who can create sales and invoicing documents which are posted into the sell-in application in Channel Sales Management for Hi-Tech in the CRM system.</td>
</tr>
<tr>
<td>ERP backend</td>
<td></td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory. User used for data exchange between CRM and ERP. Depending on RFC destination, the user can be an individual user or a system RFC user. Created by R/3 system administrator.</td>
</tr>
</tbody>
</table>

Authorizations

Channel Sales Management for Hi-Tech uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP [Extern] also apply to the application.

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

In addition to this Channel Sales Management for Hi-Tech uses the Business Partner information in the CRM system to determine the authorizations of a user. This is done by...
maintaining the business partners in different roles and assigning these partners to the end users. Refer to the sections below for further details.

**Standard Roles**
The table below shows the standard roles that are used by Channel Sales Management for Hi Tech.

**Standard Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM Business Partner Role – Employee</td>
<td>For more information, see SAP OSS Note 715494</td>
</tr>
<tr>
<td>CRM Business Partner Role – Contact Person, Internet User</td>
<td>For more information, see SAP OSS Note 715494</td>
</tr>
</tbody>
</table>

**Standard Authorization Objects**
The table below displays the security-relevant authorization objects that are used by Channel Sales Management for Hi-Tech.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS_SGEN</td>
<td>ACTVT</td>
<td>01,03</td>
<td>Generation of Rule Schema</td>
</tr>
<tr>
<td>CMS_SMAINT</td>
<td>ACTVT</td>
<td>01,03</td>
<td>Maintenance of Rule Schema</td>
</tr>
<tr>
<td>CMS_CIR</td>
<td>CHNL_PART, SALES_ORG</td>
<td>ACTVT</td>
<td>*</td>
</tr>
<tr>
<td>CMS_MPBM</td>
<td>ACVT</td>
<td>01,02,03</td>
<td>Maintenance of Channel Inventory data</td>
</tr>
<tr>
<td>CMS_IR</td>
<td>CHNL_PART, SALES_ORG</td>
<td>ACTVT</td>
<td>*</td>
</tr>
<tr>
<td>CMS_RT_AUT</td>
<td>CHNL_PART, SALES_ORG</td>
<td>ACTVT</td>
<td>*</td>
</tr>
<tr>
<td>CMS_PP_AUT</td>
<td>CHNL_PART, SALES_ORG</td>
<td>*</td>
<td>Generation and Processing of Price Protection data</td>
</tr>
</tbody>
</table>
Network and Communication Security

The network topology for Channel Sales Management for Hi Tech 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 Network and Communication Security chapter also apply to Channel Sales Management for Hi Tech. Details that specifically apply to the application are described in the following topics:

- Communication Channel Security
  
  This topic describes the communication paths and protocols used by Channel Sales Management for Hi Tech.

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

- Network and Communication Security
- Security Aspects for Connectivity and Interoperability

Communication Channel Security

The various communication channels that are used between the components of Channel Sales Management for Hi Tech and other applications are listed in the following table:

### Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to SAP Enterprise Portal</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>mySAP CRM server to SAP ERP server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>SAP ERP server to mySAP CRM server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and ERP data</td>
</tr>
<tr>
<td>mySAP CRM server to IPC</td>
<td>RFC</td>
<td>Pricing conditions</td>
<td>System information and CRM data</td>
</tr>
</tbody>
</table>
mySAP CRM server to third-party supplier (TTE or Vertex) | RFC | Tax data | System information and CRM data

The following figure illustrates the communication paths mentioned above:
Contracts and Chargeback for Pharmaceutical

Introduction
SAP CRM Contracts and Chargeback for Pharmaceuticals is an ABAP based solution. It encapsulates the following functions which have been modeled as different applications.

- Contracts Management
- Chargeback Claims Processing
- Sell-In (Sales to Channel Partner)
- Transmission Management

These applications enable processing of the Contracts & Chargeback data, which also includes creation of sales documents in the CRM system and sales and invoicing documents in the back-end ERP system.

This chapter provides the security information for Contracts and Chargeback for Pharmaceuticals.

Why Is Security Necessary?
Security is necessary, because Contracts and Chargeback for Pharmaceuticals:

- Accesses data in the CRM system, such as contract price information, member eligibility information, and chargeback claims related information which is maintained in the CRM system
- Leads to creation of sales documents in the CRM (which are replicated and invoiced in the backend ERP system)

Therefore, it is very important to restrict access to this data.

User Administration and Authentication
Contracts and Chargeback for Pharmaceuticals uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology [Extern] also apply to the Contracts and Chargeback for Pharmaceuticals application.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to Contracts and Chargeback for Pharmaceuticals in the following topic:

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with Contracts and Chargeback for Pharmaceuticals.

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

User Management Tools

<table>
<thead>
<tr>
<th>Tools</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance</td>
<td>For more information, see</td>
<td></td>
</tr>
</tbody>
</table>
with SAP Web AS ABAP (Transactions SU01, PFCG) | Users and Roles (BC-SEC-USR).

### User Types

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM System</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory. User who can access Contracts and Chargeback transactions. Created by CRM system administrator.</td>
</tr>
<tr>
<td>CRM System</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory. User who can process background jobs.</td>
<td></td>
</tr>
<tr>
<td>ERP backend</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory. User who can create sales and invoicing documents which are posted into the sell-in application in Contracts and Chargeback for Pharmaceuticals in the CRM system.</td>
</tr>
<tr>
<td>ERP backend</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory. User used for data exchange between CRM and ERP. Depending on RFC destination, user can be individual user or system RFC user. Created by R/3 system administrator.</td>
<td></td>
</tr>
</tbody>
</table>

### Authorizations

Contracts and Chargeback for Pharmaceuticals uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP [Extern] also apply to the application.

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

In addition to this Contracts and Chargeback for Pharmaceuticals uses the Business Partner information in the CRM system to determine the authorizations of a user. This is done by maintaining the business partners in different roles and assigning these partners to the end users. Refer to the sections below for further details.

### Standard Roles

The table below shows the standard roles that are used by Contracts and Chargeback for Pharmaceuticals.
Role Description

Portal Role – Chargeback Analyst (SAP_PCC_CMS_CB_ANALYST)

Technical name: com.sap.pct.ispha.nfp.chargebackanalyst
For more information, see SAP Service Marketplace at service.sap.com/securityguide
→ SAP Enterprise Portal (EP) Security Guides

Portal Role – Contract Administrator (SAP_PCC_CMS_CNTR_ADMIN)

Technical name: com.sap.pct.ispha.nfp.contractadmin
For more information, see SAP Service Marketplace at service.sap.com/securityguide

CRM Business Partner Role – Employee
For more information, see SAP OSS Note 715494.

CRM Business Partner Role – Contact Person, Internet User
For more information, see SAP OSS Note 715494.

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by Contracts and Chargeback for Pharmaceuticals.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS_SGEN</td>
<td>ACTVT</td>
<td>01,03</td>
<td>Generation of Rule Schema</td>
</tr>
<tr>
<td>CMS_SMAINT</td>
<td>ACTVT</td>
<td>01,03</td>
<td>Maintenance of Rule Schema</td>
</tr>
<tr>
<td>CMS_CBAUTH</td>
<td>CHNL_PART</td>
<td>*</td>
<td>Processing and maintenance of Chargeback claims data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>02,03,43</td>
<td></td>
</tr>
<tr>
<td>CMS_SI_AUT</td>
<td>CHNL_PART</td>
<td>*</td>
<td>Processing and maintenance of Sell-In data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>02,03,43</td>
<td></td>
</tr>
<tr>
<td>CMS_TO</td>
<td>PARTNER</td>
<td>*</td>
<td>Maintenance of transmission data</td>
</tr>
<tr>
<td></td>
<td>ACVT</td>
<td>02</td>
<td></td>
</tr>
</tbody>
</table>

Network and Communication Security

The network topology for Contracts and Chargeback for Pharmaceuticals 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 Network and Communication Security [Extern] chapter also apply to Contracts and Chargeback for Pharmaceuticals. Details that specifically apply to the application are described in the following topics:

Communication Channel Security

This topic describes the communication paths and protocols used by Contracts and Chargeback for Pharmaceuticals.

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

- Network and Communication Security
Security Aspects for Connectivity and Interoperability

**Communication Channel Security**

The various communication channels that are used between the components of Contracts and Chargeback for Pharmaceuticals and other applications are listed in the following table:

### Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to SAP Enterprise Portal</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>mySAP CRM server to SAP ERP server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>SAP ERP server to mySAP CRM server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and ERP data</td>
</tr>
<tr>
<td>mySAP CRM server to IPC</td>
<td>RFC</td>
<td>Pricing conditions</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to third-party supplier (TTE or Vertex)</td>
<td>RFC</td>
<td>Tax data</td>
<td>System information and CRM data</td>
</tr>
</tbody>
</table>

The following figure illustrates the communication paths mentioned above:
Lead Management with Channel Management

The leads with Channel Management and its partner information are stored without access control. In the lead-application it is possible to see all leads and to choose every partner related to the lead.

Authorizations

In the channel management scenario, the maintenance and visibility of leads depend on the portal role of the user.

In the role partner manager, the user is allowed to see and maintain leads that are assigned to the partner manager or to one of his employees.

In the role partner employee, the user is only allowed to see leads and should only be able to set partners in the lead, he is allowed to.

Therefore the access via a portal application has to be controlled by the Access Control Engine with the help of rules that are designed for special roles.

You will find further information about the access control rules for leads in channel management on SAP Help Portal under help.sap.com → Dokumentation → mySAP Business Suite → SAP Customer Relationship Management → Channel Management → Channel Marketing → Lead Processing with Channel Partner → Basic Functions → CRM Access Control Engine > Access Control Rules for Leads

It has to be ensured that all necessary rules in the ACE-environment have to be activated:

Partner Manager Role:

- LEAD_PARTNER_MAN
- LEAD_CHP_PROSP_MAN
- LEAD_CHP_EMP_RES_MAN
- LEAD_CHP_CP_MAN
- LEAD_CHPENDCUST_MAN
- LEAD_WFINB_PARTMANAG

Partner Employee Role:

- LEAD_PARTNER_EMP
- LEAD_CHP_PROSP_EMP
- LEAD_CHP_EMP_RES_EMP
- LEAD_CHP_ENDCUST_EMP
- LEAD_CHP_CP_EMP

Checklist

Here you find a checklist with the features, their security settings and how you can prove them.
### Checklist

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control access of leads for different partner roles</td>
<td>Are rules activated?</td>
<td>You find the menu to check at Customizing under Customer Relationship Management → Channel Management → Basic Settings → Access Control Engine → ACE_ACTIVATION, Tab Monitoring if all necessary rights have the status ACTIVE.</td>
</tr>
</tbody>
</table>
Introduction

SAP CRM Billing is a ABAP based application that enables creating customer invoices in SAP CRM. The CRM Billing application is integrated in CRM Enterprise scenarios.

The billing documents and the actual revenues can be posted in Financial Accounting and in Controlling of SAP ERP by using the standard integration between CRM Billing and ERP FI / CA modules.

This chapter describes the security information for CRM Billing.

Why Is Security Necessary?

Security is necessary, because CRM Billing:

- accesses data in the CRM system, such as business partner information, and consists business data information, such as invoices;
- has direct access to the pricing engine where all products and prices are stored and to the tax engine as well;
- has integration to ERP FI module which is very important for the whole financial services.

Therefore, it is very important to restrict access to this data.

User Administration and Authentication

The CRM Billing uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology also apply to the CRM Billing application. For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → SAP Web Application Server Security Guide → SAP Web AS for ABAP Technology.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to the CRM Billing at User Management [Seite 25].

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the CRM Billing application.

User Management

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

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Web AS ABAP (Transactions SU01, PFCG)</td>
<td>For more information, see SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 04 → English → SAP Library</td>
<td></td>
</tr>
</tbody>
</table>
The following users must be created for the CRM Billing:

### User Types

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRMSystem</td>
<td>End User</td>
<td>No</td>
<td>Dialog User</td>
<td>No</td>
<td>Mandatory User who can access Billing transactions. Created by CRM system administrator</td>
</tr>
<tr>
<td>CRMSystem</td>
<td></td>
<td>No</td>
<td>System User</td>
<td>No</td>
<td>Mandatory User who can process background jobs</td>
</tr>
<tr>
<td>ERP Backend</td>
<td></td>
<td>No</td>
<td>System User</td>
<td>No</td>
<td>Mandatory User used for data exchange between CRM and ERP. Depending on RFC destination, user can be individual user or system RFC user. Created by R/3 system administrator.</td>
</tr>
<tr>
<td>CRMSystem</td>
<td>IPC User</td>
<td>No</td>
<td>System User</td>
<td>No</td>
<td>Mandatory User for communication with IPC Server</td>
</tr>
</tbody>
</table>

### Authorizations

CRM Billing uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP also apply to the application.

The SAP Web Application Server authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the SAP Web AS ABAP.
Standard Roles
The table below shows the standard roles that are used by CRM Billing.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal Role - Billing Clerk</td>
<td>For more information about the Business Package for SAP CRM, see SAP Help Portal under help.sap.com → Documentation → mySAP Business Suite → Customer Relationship Management → Roles → Business package for SAP CRM 5.0</td>
</tr>
<tr>
<td>Portal Role - Sales Assistant/Sales Manager</td>
<td>For more information about the Business Package for SAP CRM, see SAP Help Portal under help.sap.com → Documentation → mySAP Business Suite → Customer Relationship Management → Roles → Business package for SAP CRM 5.0</td>
</tr>
</tbody>
</table>

Standard Authorization Objects
The table below shows the security-relevant authorization objects that are used by CRM Billing.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEA_DLI</td>
<td>ACTVT, APPL, BILL_ORG, BILL_TYPE</td>
<td>Maintenance of the billing due list</td>
</tr>
<tr>
<td>BEA_BDH</td>
<td>ACTVT, APPL, BILL_ORG, BILL_TYPE</td>
<td>Creation and maintenance of billing</td>
</tr>
<tr>
<td>BEA_SUBS</td>
<td>ACTVT, APPL, BILL_TYPE</td>
<td>Display of documents in SAP R/3</td>
</tr>
</tbody>
</table>

Network and Communication Security
The network topology for CRM Billing is based on the topology used by the SAP NetWeaver platform and CRM Middleware. Details that specifically apply to the application are described in Communication Channel Security [Seite 40].

This topic describes the communication paths and protocols used by CRM Billing.

- For more information, see the following sections in the SAP NetWeaver Security Guide at the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide →

**Communication Channel Security**

Given below are the various communication channels that are used between the components of CRM Billing and other applications:

### Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP/HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to SAP Enterprise Portal</td>
<td>HTTP/HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>mySAP CRM server to SAP ERP server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>SAP ERP server to mySAP CRM server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and ERP data</td>
</tr>
<tr>
<td>mySAP CRM server to SAP BW server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to IPC</td>
<td>RFC</td>
<td>Pricing conditions</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to third-party supplier (TTE or Vertex)</td>
<td>RFC</td>
<td>Tax data</td>
<td>System information and CRM data</td>
</tr>
</tbody>
</table>
In most cases, only application data is sent across (Billing Due List DLI and Billing Document BDH/BDI). The data that is received is:

- Deliveries from SAP R/3
- Orders from CRM Sales
- Status feedback from FI
**CRM Rebates**

**Introduction**

This topic describes the security information for CRM Rebates.

**Why Is Security Necessary?**

Security is necessary, because CRM Rebates:

- accesses data in the CRM system, like CRM Billing, such as business partner information, and consists business data information, such as invoices;
- has direct access to the pricing engine where all products and prices are stored and to the tax engine as well;
- has integration to ERP FI module which is very important for the whole financial services.

Therefore, it is very important to restrict access to this data.

**User Administration and Authentication**

The CRM Rebates uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology [Extern] also apply to the CRM Rebates application.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to the CRM Rebates in [User Management][1].

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the CRM Rebates application.

**User Management**

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

**User Management Tools**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Web AS ABAP (Transactions SU01, PFCG)</td>
<td>For more information, see the SAP Help Portal under help.sap.com→Documentation→SAP NetWeaver→SAP NetWeaver 04→English→SAP Library→SAP NetWeaver→Security→Identity Management→Users and Roles (BC-SEC-USR)</td>
<td></td>
</tr>
</tbody>
</table>

The following users must be created for the CRM Rebates:

**User Types**
<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>No</td>
<td>Mandatory User who can access Rebates transactions. Created by CRM system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td></td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory User who can process background jobs</td>
</tr>
<tr>
<td>ERP back end</td>
<td></td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory User used for data exchange between CRM and ERP. Depending on RFC destination, user can be individual user or system RFC user. Created by R/3 system administrator.</td>
</tr>
<tr>
<td>CRM system</td>
<td>IPC user</td>
<td>No</td>
<td>System user</td>
<td>No</td>
<td>Mandatory User for communication with IPC Server</td>
</tr>
</tbody>
</table>

### Authorizations


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

### Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by CRM Price list.
Standard Authorization Objects

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEA_RDLH</td>
<td>ACTVT</td>
<td>Maintenance of the rebates due list</td>
</tr>
<tr>
<td></td>
<td>APPL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BILL_ORG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REB_PROF</td>
<td></td>
</tr>
<tr>
<td>BEA_RPDH</td>
<td>ACTVT</td>
<td>Creation and maintenance of rebate settlement documents</td>
</tr>
<tr>
<td></td>
<td>APPL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BILL_ORG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SETTL_TYPE</td>
<td></td>
</tr>
<tr>
<td>BEA_REXH</td>
<td>ACTVT</td>
<td>Creation and maintenance of rebate extracts</td>
</tr>
<tr>
<td></td>
<td>APPL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BILL_ORG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EXTCT_TYPE</td>
<td></td>
</tr>
<tr>
<td>CRM_RBAG</td>
<td>ACTVT</td>
<td>Creation and maintenance of rebate agreements</td>
</tr>
</tbody>
</table>

Network and Communication Security

The network topology for CRM Rebates 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 at the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Network and Communication Security and Security Aspects for Connectivity and Interoperability also apply to CRM Rebates. Details that specifically apply to the application are described in Communication Channel Security [Seite 40].

This topic describes the communication paths and protocols used by CRM Price list.

Communication Channel Security

Given below are the various communication channels that are used between the components of CRM Rebates and other applications:

Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
</tbody>
</table>
In most cases, only application data is sent across (Rebate Extracts REXH/REXI/RCON and Rebate Settlement Documents RPDH/RPD1). The data that is received is:

- Billing documents from CRM Billing
- Rebate Agreements from CRM Sales
- Status feedback from FI
SAP CRM Powered by SAP NetWeaver
### CRM Server

#### Introduction

This section explains the security aspects associated with the data present in the CRM server. The CRM Middleware, which is an integral part of the CRM server, is based on the following components:

- CRM Server
- R/3 Backend System

#### Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
</table>

#### Why Is Security Necessary?

The data synchronization within the CRM landscape (CRM Server, R/3 Backend System, Connectivity to BW and CRM Mobile Clients) is provided by the CRM Middleware. 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 as a critical topic and must be considered while setting up and customizing the system landscape. It is required to establish a well-defined authorization concept which assigns the appropriate roles with restricted authorizations to the different user groups in your company (examples: users and administrators of the administration console have different roles, system administrator has full access to the queue monitors and the restart ability and deletion in the BDoc message monitoring tools). Information related to this topic can be found in the following sections.

#### Important SAP Notes

⚠️ Check the SAP Notes that are applicable to the security of the application on a regular basis.

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>338537</td>
<td>RFC user authorization for data exchange between R/3 back end &lt;-&gt; CRM</td>
<td>This note provides some recommendations on how to define the authorization concept for the data exchange between the R/3 Backend system and CRM Server. This is applicable to the main applications.</td>
</tr>
</tbody>
</table>
User Administration and Authentication

User Management

The data synchronization between the CRM Server and R/3 Backend and within the CRM Server itself is based on the RFC protocol. To enable the RFC connection between two systems/clients, a user is required. The use of a communication user (also known as RFC user) is very important in 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 details, see SAP Note 338537 for up-to-date information on CRM user authorizations. The following table lists the users that must be created to enable the data exchange.

**Standard Users**

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
</table>
| R/3 Backend System | User to the CRM Server and client             |            | Communication user | To be set by the administrator | Refer to the IMG documentation under:  
Customer Relationship Management  
→ CRM Middleware and Related Components  
→ Communication Setup  
Create RFC Users.                                                                                                                                    |
| CRM Server         | User to the R/3 Backend and client            |            | Communication user | To be set by the administrator | Refer to the IMG documentation under:  
Customer Relationship Management  
→ CRM Middleware and Related Components  
→ Communication Setup  
Create RFC Users.                                                                                                                                    |
| CRM Server         | Replication and realignment user              |            | Communication user | To be set by the administrator | Refer to the IMG documentation under:  
Customer Relationship Management  
→ CRM                                                                                                                                                |
Authorizations

The CRM middleware delivers different roles that are assigned to, Middleware administrator, Middleware developer, 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. It is recommended to have well-defined roles at the first phase of the project. It is important to assign to the system responsible and to the SAP Support users with full access to the main tools and transactions. The roles delivered by SAP are described in the following sections.

General CRM Middleware Roles

The following table lists the composite roles that are available for CRM Middleware:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_MW_ADM</td>
<td>SAP CRM Middleware Administrator</td>
</tr>
<tr>
<td></td>
<td>This role allows you to start all the transactions associated with the administration of the CRM server. This role is assigned to the CRM Middleware Administrator or SAP Support staff. However, to ensure proper system monitoring, this role must be granted only to system administrators in the productive systems.</td>
</tr>
<tr>
<td>SAP_CRM_MW_CUSTOMIZING</td>
<td>Customizing steps for CRM Middleware (single role)</td>
</tr>
<tr>
<td></td>
<td>This role allows you to customize the CRM Middleware. This role is assigned to consultants and is primarily required during the initial setup of the CRM server.</td>
</tr>
<tr>
<td>SAP_CRM_MW_DEV</td>
<td>SAP CRM Middleware Developer</td>
</tr>
<tr>
<td></td>
<td>This role is primarily required in the development system. However, during a crisis situation, this role can be used in the production system.</td>
</tr>
</tbody>
</table>

Each role contains single roles. For details, refer to Role Maintenance (transaction PFCG).

The transactions along with their assigned roles are explained as follows:

BDoc Summary, Transactions R3AC1, R3AC3, R3AC5

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_MW_ADP_ADMINISTRATOR</td>
<td>Authorizations for starting an initial load</td>
</tr>
<tr>
<td>SAP_CRM_MW_ADP_CUSTOMIZER</td>
<td>Authorizations for transaction codes R3AC1, R3AC3, and R3AC5</td>
</tr>
</tbody>
</table>
BDoc Modeler, Transaction SBDM

The following table lists the roles that SAP delivers:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_BDM_ACTIVATE_ALL</td>
<td>BDoc Modeler – Activate all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_CHANGE_ALL</td>
<td>BDoc Modeler – Change all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_CHECK_ALL</td>
<td>BDoc Modeler – Check all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_DELETE_ALL</td>
<td>BDoc Modeler – Delete all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_DISPLAY_ALL</td>
<td>BDoc Modeler – Display all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_GENERATE_ALL</td>
<td>BDoc Modeler – Generate all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_RELEASE_ALL</td>
<td>BDoc Modeler – Release all BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_SYNC_BDOCS</td>
<td>BDoc Modeler – Synchronization BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_MESSAGING_BDOCS</td>
<td>BDoc Modeler – Messaging BDoc types</td>
</tr>
<tr>
<td>SAP_CRM_BDM_MOBILE_APPL_BDOCS</td>
<td>BDoc Modeler – Mobile Application BDoc types</td>
</tr>
</tbody>
</table>

BDoc message Summary, transaction SMW01

BDoc messages are data containers used during the data synchronization by the CRM Middleware. 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 SMW01. It is recommended to restrict the access to the transaction SMW01 in the production system to the system administrators, SAP Support and to the responsible project leads or members only. Remove the authorizations for transaction SMW01 for all the other dialog users. Developers have usually full access to the development and test systems. It is also recommended to restrict the authorizations to the use of the reprocess 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>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_MWSMW_DELETE</td>
<td>Check authorization to delete BDoc messages</td>
</tr>
<tr>
<td>SAP_CRM_MWSMW_RETRY</td>
<td>Check authorization to retry the processing of BDoc messages</td>
</tr>
</tbody>
</table>

QRFC Queues, Transactions SMQ1 / SMQ2

To optimize the use of the system resources and the parallelization of the data processing, the data synchronization uses the SAP Basis queue mechanisms. The data is partly readable in the queues. You must prevent access to the data in these qRFC queues. To do this, remove authorizations for transactions SMQ1 and SMQ2 for all the dialog users. Only administrators, CRM project responsible and SAP Support need to start these transactions. The deletion of queue entries is also very critical (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. Refer to note 93254 for the activation of the authorization check for the deletion from the RFC queues.

Follow also the instructions provided in note 622722. This ensures that the Inbound Queues are processed by a user with the required authorizations. For all the other dialog users, differentiate between power users who are aware of the consequences of deleting a queue entry or putting stop entries.

R&R Queue Processing, transaction SMOHQUEUE

This section is valid for the scenario field applications only. If the processing of the Replication and Realignment queues (provide data to the mobile clients) extends for a long period of time,
do not delete the entries present in the queues. Subsequently, 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 the data distribution are caused by customers
due to unauthorized interference in the queue processing, then SAP is not responsible for
these inconsistencies. SAP recommends stringent measures to be followed before assigning
authorizations for the SMOHQUEUE transaction. 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 the single authorizations objects are
required. The following table lists the relevant authorization objects.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_MW_FC</td>
<td></td>
<td></td>
<td>Flow control</td>
</tr>
<tr>
<td>CMW_BDM</td>
<td></td>
<td></td>
<td>BDoc Modeler</td>
</tr>
<tr>
<td>CMW_CRMADP</td>
<td></td>
<td></td>
<td>CRM Adapter Repository</td>
</tr>
<tr>
<td>CMW_GEN</td>
<td></td>
<td></td>
<td>CRM Middleware Generation</td>
</tr>
<tr>
<td>CRM_MW_AC</td>
<td></td>
<td></td>
<td>Admin Console</td>
</tr>
<tr>
<td>CRM_MW_BDM</td>
<td></td>
<td></td>
<td>BDoc Modeler</td>
</tr>
<tr>
<td>CRM_MW_DC</td>
<td></td>
<td></td>
<td>Data Collector/Extractor</td>
</tr>
<tr>
<td>CRM_MW_RR</td>
<td></td>
<td></td>
<td>R&amp;R queue administration</td>
</tr>
</tbody>
</table>

The fields, values of these objects, and their description can be found in the online
documentation that is available on the CRM Server.

**Network and Communication Security**

**Communication Destinations**

**Connection Destinations**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivered?</th>
<th>Type</th>
<th>User, Authorizations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC destinations for the R/3 target systems (R/3 Backend, BW, APO)</td>
<td>No</td>
<td>RFC connection</td>
<td>Refer to the IMG documentation under: Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Create RFC Users.</td>
<td>Refer to the IMG documentation under: Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Define RFC Destinations. For more information, see note 338537.</td>
</tr>
<tr>
<td>RFC destinations for non-R/3</td>
<td>No</td>
<td>RFC Destination</td>
<td>Refer to the IMG documentation</td>
<td>Refer to the IMG documentation</td>
</tr>
</tbody>
</table>
Checklist

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data synchronization in the system landscape</td>
<td>RFC destinations and RFC users</td>
<td>Refer to Communication Destinations and User Management</td>
</tr>
<tr>
<td>Authorization concept</td>
<td>Roles and authorization objects assigned to the different user groups</td>
<td>Refer to Authorizations and Standard authorization objects</td>
</tr>
<tr>
<td>Data protection and consistency</td>
<td>BDoc messages: SMW01 Queuing: SMQ1 and SMQ2 Data replication: SMOHQUEUE (For field applications only)</td>
<td>Refer to BDoc messages summary, qRFC Queues, and R&amp;R queuing</td>
</tr>
</tbody>
</table>

Target Systems

under: Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Create RFC Users.

under: Customer Relationship Management → CRM Middleware and Related Components → Communication Setup → Define RFC Destinations.
Software Agent Framework

Introduction
This guide is for the compilation service and search service of the Software Agent Framework (application component CRM-BF-SAF).

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most-Relevant Sections or Specific Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interaction Center (IC) WebClient</td>
<td>SAP Customer Relationship Management (CRM) security guide</td>
<td>[Interaction Center WebClient Seite 163]</td>
</tr>
<tr>
<td>Search and Classification (TREX)</td>
<td>SAP Knowledge Management security guide</td>
<td>[Search and Classification (TREX) Security Guide Seite 163]</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?
Data protection is important for this application because the 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 transaction SU01.

User

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed Description</th>
</tr>
</thead>
</table>
| CRM    | Knowledge engineer | No         | Dialog | No               | There are different ways to access the SAF’s Indexes BSP application:  
To access via URL or from the CRM system directly, a standard CRM user is sufficient.  
To access from SAP Enterprise Portal, the user must have access to CRM Portal Administrator |
Network and Communication Security

Communication Channel Security
TREX’s ABAP application programming interface (API) communicates with the TREX server via TCP/IP communication supported by SAP’s standard RFC definition. In the Knowledge Management Security Guide, see Search and Classification (TREX) Security Guide [Extern].

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 the CRM system in Customizing for the 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 functionality. Furthermore, any content access through a business application via the SAF, such as view details, is controlled by individual business objects, such as problem and solution in the Solution Database (SDB).

Access control can be administrated by SAP’s standard authorization and SAF information security. For details on SAF information security, see:

- Generic Information Security on SAP Help Portal under mySAP Customer Relationship Management
- Customizing for the Software Agent Framework (Customer Relationship Management → Enterprise Intelligence → Software Agent Framework) → Business Add-Ins (BAdIs) → BadI: Information Security

<table>
<thead>
<tr>
<th>Stored Data</th>
<th>Stored Where</th>
<th>Stored When</th>
<th>Type of Access</th>
<th>Protected by Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge bases</td>
<td>SAP system</td>
<td>Knowledge base maintenance</td>
<td>Read/write/delete/change</td>
<td>Yes - Access to CRM system</td>
</tr>
<tr>
<td>Knowledge base indexes (compilation service)</td>
<td>TREX</td>
<td>Indexing</td>
<td>Write/delete/change</td>
<td>Yes – Access required to Indexing/Clustering/TREX server</td>
</tr>
<tr>
<td>Knowledge base indexes (search service)</td>
<td>TREX</td>
<td>User interaction</td>
<td>Read</td>
<td>Yes – Access required to CRM/TREX server</td>
</tr>
<tr>
<td>Compilation status/time stamp</td>
<td>SAP system</td>
<td>Indexing/clustering</td>
<td>Read/write/delete/change</td>
<td>Yes - Access to Indexes BSP application</td>
</tr>
<tr>
<td>Clustering result</td>
<td>SAP system</td>
<td>Clustering</td>
<td>Read/write/delete/change</td>
<td>Yes - Access to Clustering result</td>
</tr>
<tr>
<td>SAF Customizing</td>
<td>CRM system</td>
<td>SAF post installation</td>
<td>Read/write/delete/change</td>
<td>Yes - Access required to Customizing application</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Feedback (search service)</td>
<td>CRM system</td>
<td>User interaction</td>
<td>Read/write/change</td>
<td>Yes - Access required to Customizing application</td>
</tr>
</tbody>
</table>

There are no other places in which data is temporarily stored.

The compilation service supports/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.
Solution Database

Introduction

This section covers the Solution Database (application component CRM-MD-SDB).

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most Relevant Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Agent Framework</td>
<td>SAP Customer Relationship Management (CRM) security guide</td>
<td>Software Agent Framework [Seite 221]</td>
</tr>
<tr>
<td>Content Management</td>
<td>SAP Knowledge Management security guide</td>
<td>Content Management Security Guide [Extern]</td>
</tr>
</tbody>
</table>

Why Is Security Necessary?

Certain kinds of information that can be stored in the Solution Database (SDB) should not be accessible to all, such as company data and employee data. Therefore, it is necessary to restrict access to certain information. In the SDB itself, problem and solution records can be accessed only via the SDB’s search interface. When the SDB is searched from another application (for example, from the Interaction Center 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 via information security. For details on information security, see User Management below.

Important SAP Notes

⚠️ Check regularly which SAP Notes are available about the security of the application.

User Administration and Authentication

User Management

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain Information Security Profile</td>
<td>See below</td>
</tr>
<tr>
<td>(transaction CRMD_SDB_PRMN)</td>
<td></td>
</tr>
<tr>
<td>Assign Profile to User</td>
<td>See below</td>
</tr>
<tr>
<td>(transaction CRMD_SDB_PROF)</td>
<td></td>
</tr>
</tbody>
</table>

Solution Database (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 via:

- Knowledge search in Interaction Center (IC) WebClient
- Knowledge search in IC WinClient
- Standalone 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 Solution Database via 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>
<thead>
<tr>
<th>Problem Profile</th>
<th>Solution Profile</th>
<th>Group Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual profile containing a set of values for one or more of the following attributes:</td>
<td>Individual profile containing a set of values for one or more of the following attributes:</td>
<td>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</td>
</tr>
<tr>
<td>• Problem type</td>
<td>• Solution type</td>
<td></td>
</tr>
<tr>
<td>• Problem subtype</td>
<td>• Solution subtype</td>
<td></td>
</tr>
<tr>
<td>• Application area</td>
<td>• System status</td>
<td></td>
</tr>
<tr>
<td>• Validation category</td>
<td>• User status</td>
<td></td>
</tr>
<tr>
<td>• Priority type and level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• System status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• User status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Subject profile</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There is no additional user management for information security. The standard SAP users are employed. 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.

### Network and Communication Security

There are no special network and communication security requirements because it is sufficient that security is ensured by default settings.

### Data Storage Security

There are no special data storage security requirements because it is sufficient that security is ensured by default settings.

Solution Database records are stored in the database of the SAP system as master data. Individual information security profiles and group information security profiles are stored and delivered as customized data of the SDB (see User Management).

### Other Security-Relevant Information

This application does not use active code on the front end.
People-Centric User Interface

User Administration and Authentication

User Management

- You must create and store all users in the CRM Server and the backend system. All customers must first have an account to use web applications

  User management is not handled by the People-Centric UI framework or by the web applications that use the People-Centric UI.

- User authentication is performed by the SAP Web Application Server along with the connected SAP R/3 system (CRM Server).

Integration Into Single Sign-On Environments

Single Sign-On (SSO) is not handled by the People-Centric UI framework.

Authorizations

The main controller of the People-Centric UI framework performs the authority check. The authority check is performed on the object BSP_APPL. This object contains the following fields:

- BSP_APPL: Handles access to all kinds of BSP applications
- BSP_VIEW: Handles access to certain views for applications in the People-Centric UI

The authority check is performed on this object only when the People-Centric UI is initialized.

Be careful with the authorization object BSP_APPL because if a user has asterisk (*) as value, then he can start every PC-UI application by internet.

There is a special trace available for PC-UI applications so that you can see the possible authorization objects that can be given to a role. This can be done in transaction PFCG on the menu tab (Choose the external service PC-UI and search for the application view name.)

For more information about authority checks and working with authorization objects, see:


Network and Communication Security

Communication Channel Security

The SAP Web Application Server must be directly accessible to all portal clients to ensure that People-Centric UI framework functions as required.
The table below shows the general communication paths used, the protocol used for the connection, and the type of data transferred.

**Communication Technology**

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of data transferred</th>
<th>Data Requiring special protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser to application</td>
<td>HTTP/HTTPS</td>
<td>All application data</td>
<td>Passwords and other sensitive data</td>
</tr>
<tr>
<td>mySAP CRM server to mySAP CRM server/ SAP R/3 server</td>
<td>RFC</td>
<td>system ID, client, and host name, all application data</td>
<td>System information and application data</td>
</tr>
</tbody>
</table>

**Secure Socket Layer (SSL)**

The interaction between the People-Centric UI framework and SSL is limited. You use SSL to extend the functionality of HTTP.

The SAP Web Application Server functions and SSL do not interact with the web applications running in the browser, nor does it affect the People-Centric UI framework, which is used by these applications. However, each controller of the People-Centric UI framework must be registered to be able to use HTTPS. To do this, you must:

- Open the PC UI framework CRM_BSP_FRAME, using the transaction SE80.
- Choose the Controllers folder from the navigation bar and double-click on one of the listed controllers, e.g. for the controller address.do, choose the checkbox HTTPS under Transfer Options.

![Tip](TipIcon.png)

To use SSL on the SAP Web AS with the People-Centric UI framework, you must perform this action for each and every controller of the framework.

**Level of Protection**

The People-Centric UI framework handles only one security level and that is for the configuration data. The security of the connections is managed by the web applications using the People-Centric UI framework, and not by the framework itself.

The URL connection to the backend 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 People-Centric UI. The People-Centric 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 via HTTP POST

When using the People-Centric UI, it is recommended that you disable the CRM Designer connection. This can be done using the SCIF transaction. In addition, you can also switch the framework and server into SSL mode.

**Minimal Installation**

A user with SAP_ALL rights can call applications that are not part of the portal. To restrict this, do the following:

1. Blueprint Customizing, using the transaction CRMC_BLUEPRINT.
2. Choose **Layout of User Interface** → **Application/Layout**.
In the edit mode you can remove the application from the list.

In case you want to add this application to the list at a later point in time, you must re-enter all the settings of the application layout.

Other Security-Related Information

People-Centric UI Framework Components Using JavaScript

- Search Result List (Searchres.do)
  The Result List classes generate JavaScript for creating HREF links. Links will be generated only when the Result List is used for portals.

- Value Help: Uses JavaScript in cases when:
  - All tags for using Value Help are rendered
  - The customer triggers value help, JavaScript will take care of creating a browser window and handles the selections the user creates.

  Value Help is not available when JavaScript is switched off.

  Results list as hierarchy (Searchret.do) and find (Searchreq.do) uses JavaScript to launch the Popup-to-Confirm. If you deactivate JavaScript, then you cannot use these components because without the Popup-to-Confirm, the chain of execution for saving changed or new data is broken.

- Interface Object Link Generation
  The interface calls the object link generation method and gets the JavaScript, which is then executed on the browser. If you do not use the active code, the Object Link Generation will not work and a user will not be able to navigate from one application to another.

- Cursor Setting
  The cursor setting is implemented purely in JavaScript and the generation of the JavaScript takes place in different controllers. The setting of the cursor and the check of mandatory fields will not work without activated JavaScript.

- Mandatory Field Check
  The check of mandatory fields is implemented purely in JavaScript and the generation of the JavaScript takes place in the different controllers.

- Simple Search (Tag) and Advanced Search (Tag)
  These controllers do not add any JavaScript, but instead hyperlinks to JavaScript present in the pushbuttons shown by the view. Hence, simple and advanced search will not function properly if active scripting is disabled in the browser security settings.

- List Personalization
  This will not work if active scripting is disabled. This means that the new window will not appear for the user to personalize the list.

- F1 Help
  The help link will not work if active scripting is disabled.

- Hierarchy List (Tree.do)
The Tree classes generate JavaScript to create HREF links. Links are generated only when the Tree is used in portals. JavaScript is also used to change the design of the root node and adjust the indexes of the name part of HTML tags used for the tree node.

The Tree will not function if JavaScript is deactivated and the wrong node indexes would be passed back to the server after each roundtrip.

- HTML Container
  Uses JavaScript to insert either HTML source code or a source URL into the iframe object, which is the container. The HTML Container will not work if JavaScript is deactivated.

- Dropdown List box (DDLB), Combo Box (COBX) and Time-Combo box (TIME)
  DDLB, COBX and TIME use JavaScript only when the basis tags use JavaScript. The Result List tag and Structure Edit tag do not render JavaScript for DDLB, COBX and TIME. In the case of a Multi Edit, the container of the BSP basis is used. This container also uses JavaScript to retrieve the correct values for dropdown list boxes, combo box and time-combo box. If JavaScript is deactivated, correct values for the DDLB, COBX and TIME are not put into the dropdown list.

- EventOnEnter and EventOnSearchEnter
  These are both JavaScript functions, which provide the ENTER function on the keyboard. Depending on the focus of the mouse, a server round-trip is triggered and the data is refreshed in the view.
  Both functions will not work when JavaScript is deactivated. A user will then have to use the Go button for the search in the web browser. In addition, the Refresh button will not be available.

- Structure Edit
  Uses JavaScript for creating links. If JavaScript is deactivated, the Structure Edit will not render any usable link.

- Application Log
  Uses JavaScript for the links to the message long text. If JavaScript is deactivated, long texts for messages will not be available.

- Popups
  Uses JavaScript to open and close additional window and to emulate a modal dialog. If JavaScript is deactivated, popups will not be available.

- Main Controller (Main.do): Loads the java script file Main.js.

- Detail Controller (Detail.do)
  The Detail.do classes generate JavaScript for creating HREF links. Links are generated only when the Detail.do is used in portals. If the JavaScript is deactivated, then it would not render any functioning HREF links.

- The following controllers are dependent on JavaScript, but do not generate JavaScript on their own:
  - Result List (Searchres.do)
  - Result List with Multiple Selection (multiselect.do)
  - Multi-Edit ODP (me_detail.do)

**People-Centric UI Framework Components Not Using JavaScript**

- Pager
• Pattern Interaction Layer
• Generic Data Context
• HTML Controller
• Data Binding
• Layout Generation
Calendar (ActiveX) Control

Introduction

In CRM 5.0, the People-Centric UI applications Activity Management and Activity Scheduling use Calendar control for User Interface. The Calendar control in this case is an ActiveX control that needs to be installed on each client system where the Activity applications will be run. The ActiveX control does not need any additional libraries other than those present in the installation package.

As in case of any ActiveX control, the control can only run on Windows operating system and on browsers that support ActiveX. Also the administrator should provide the user with the rights needed to run ActiveX controls.

User Administration and Authentication

User Management

The Calendar ActiveX control is used by Calendar controller for People-Centric UI [Seite 226] framework.

Authorizations

The possible scenarios for the installation and use of Calendar ActiveX in Calendar application are as follows:

- Installation via automatic download and automatic registration of ActiveX control
  
  The ActiveX control is packaged in a CAB file that is signed by SAP. This CAB file is uploaded to the MIME repository of the server. First time the calendar application is run the active X control will be downloaded and installed automatically.

- Installation via Installer
  
  A Windows Installer (*.msi) is available for the ActiveX control. The administrator can make use of this installer to install the control on each individual PC or make use of some deployment tool like Microsoft Systems Management Services (SMS) for remotely deploying the control. If the ActiveX control is preinstalled then the application will make use of the installed version of the control without causing the automatic download.

- No authorization to run ActiveX control
  
  If customer denies the use of ActiveX control then the user will not get the Calendar in the Calendar Application. The user in this case should contact the network administrator for obtaining the required rights.

  From Security-Perspective we recommend the installation of Calendar ActiveX control via 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 via 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 rendering calendar might require changes in Internet Explorer Security Settings. The Internet Explorer Security Settings should be set to Medium during the download
process. Also the user can verify if the options “Download Signed ActiveX controls” and “Run ActiveX controls and Plug-ins” are enabled in Internet Explorer Security Settings before the download process starts. These options have to be enabled if not already enabled.

Once downloaded and registered the calendar application will use that control without causing any further downloads. Only when a new version of the control is available on the server then the download and registration of the new control is initiated. This again requires that the requirements mentioned above be satisfied.

For more information refer at the SAP Help Portal under help.sap.com → SAP NetWeaver → SAP NetWeaver → People Integration → Collaboration → Administration Guide → Groupware → Installing and Configuring Calendar Connectivity → Installing and Configuring Microsoft Exchange Connectivity → Integrating MS Exchange Using Outlook Web Access → Installing and Configuring the Active-X Control

Network and Communication Security

Communication Channel Security

Refer to People-Centric UI [Seite 226] for more information on this topic.
SAP Business Information Warehouse

Security for SAP Business Information Warehouse is covered by the security guide for BW:

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most important sections or special restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Business Information Warehouse</td>
<td></td>
<td>For more information on security, see SAP Help Portal under &lt;help.sap.com&gt; → SAP NetWeaver → Release '04 → SAP NetWeaver → Information Integration → SAP Business Information Warehouse → BI Suite: Business Explorer → Integration with the SAP Enterprise Portal → Settings in SAP BW and SAP EP → Security</td>
</tr>
</tbody>
</table>
Object Links, Input Help, Core Services, and Java Lists

Introduction
The following section contains security-relevant information on the following technical components:

- Object links
- Input help
- Core Services
- Java lists

All components are based on ABAP, Java, SAP Java Connector (JCo), and Portal components, with the following exceptions:

- Input help does not contain Java coding.
- Core services and Java lists are coded exclusively in Java, although they call remote-enabled ABAP function modules (via JCo).

Object links and input help are based on URLs that support navigation to Portal content.

Security aspects that need to be considered are as follows:

- The application called: The user can only start certain applications
- Data displayed: The user cannot see / change all data

Because URLs consist only of text, it is possible for any user to create them. In this respect, full security cannot be guaranteed for link creation. It is more the responsibility of the application to protect itself from unauthorized startup or data display/change. In other words, when a user attempts to use an application for which he/she does not have authorization, the application itself is responsible for checking this. If necessary, access must be denied. If the current user is authorized to call up the application, then the application must take into account what data can be displayed, and whether it can be displayed with change authorization or as read-only. All this cannot be covered effectively by using URLs.

Java lists call function modules in the backend and display the values determined in list format. Here, the function modules must ensure that the user is allowed to call the corresponding modules and that only “allowed” data is displayed.

Core services comprise several components

- URL Dispatcher: Analogous to object links.
- Telephony: Not security-relevant because only one telephone number is dialed

  Watch out for toll charging numbers starting with 0190.

- CRM Context: Storage of user-dependent data, management of JCo connections.
- CRM Core Backend Mapper: This can be used to define specific backend connections to system aliases for individual users or user groups. The standard security rules apply to these backend systems. Data for the Core Backend Mapper is stored in the UME.
- PSID Generator: Not security-relevant.

Related Security Guides
**Application Guide Most important sections or special restrictions**

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most important sections or special restrictions</th>
</tr>
</thead>
</table>
| SAP NetWeaver Portal         | service.sap.com/securityguide                                        | Secure Communications  
Communication with Backend Systems  
Authentication  
(Authorizations)  
Single Sign-On |
|                              | SAP NetWeaver '04 Component Security Guides  
| JCo                          | service.sap.com/securityguide                                        | Network and Communication Security  
Security Aspects for Connectivity and Interoperability  
Security Guides for the SAP NetWeaver Components |
|                              | SAP NetWeaver '04 Component Security Guides  

**Why do we need Security?**

Security aspects are important for object links, input help, Context Service, and Java lists. For object links, Java lists and input help, it is important to ensure that users can only call the appropriate content and applications. These contents or changes are protected by the program logic used.

**User Administration and Authentication**

**Integration with the Single Sign-On Environment**

Single Sign-On is used, particularly for JCo calls of RFC function modules.

**Network and Communication Security**

**Communication Channel Security**

Remote calls are made to function modules in the application server. JCo is used for this.

**Communication Destinations**

JCo calls are made to the CRM Backend. Portal system alias SAP_CRM has been created for this purpose.

For more information, see SAP Help Portal under help.sap.com → mySAP Business Suite → SAP Customer Relationship Management → SAP CRM Powered by SAP NetWeaver → Application Platform → Lifecycle Management → Configuring the Business Package for mySAP CRM → System Landscape in the Portal → Maintaining an Alias in the System Landscape

**Data Storage Security**

Data for the object links are saved in the CRM backend system. Context Service saves data in the file system of the Portal server. This data is not security-relevant.
Other Security-Relevant Information

Object links use JavaScript in the frontend.
BSP Application

Introduction

The People-Centric UI from mySAP CRM is integrated with Enterprise Portal by using the Application Integrator component, which in turn is part of SAP Enterprise Portal 6.0.

The People-Centric UI of mySAP CRM itself is a framework based on templates. It is created using the technology of the Business Server Page and is based on SAP Web Application Server.

The security guides for SAP Web Application Server and SAP Enterprise Portal cover all the security-related topics and serve as a guideline for ensuring the integration of the People-Centric UI of mySAP CRM.

Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most important sections or special restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web AS</td>
<td>SAP Service Marketplace under service.sap.com/securityguide → SAP Basis / Web AS Security Guides</td>
<td></td>
</tr>
</tbody>
</table>
CRM Access Control Engine

Introduction

The Access Control Engine (ACE) is an additional authorization concept that exists in parallel to the standard SAP authorization concept. By using ACE you are able to control authorizations on object level i.e. you can give a user access to a single object.

ACE is currently used in Channel Management Scenarios and for protection of Internet Sales processes.

The Access Control Engine (ACE) is set up and managed via Customizing under Customer Relationship Management → Basic Functions → Access Control Engine.

Because ACE authorization data will be updated while runtime caused by object changes or object creation it's important to switch off the ACE when you don't like to use it. You can switch off the ACE via Customizing under Customer Relationship Management → Basic Functions → Access Control Engine → Maintain ACE Settings.

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 i.e. users might get authorizations that they should not have.

User Administration and Authentication

To assign users to ACE rights you use ACE user groups. Those user groups can contain reference users, roles and / or collective roles. Furthermore this user groups can also contain further user groups.

⚠️ Changes on roles, reference users and ACE user groups have impact on the authorization data of ACE.

After (re)activating of a corresponding right or refresh of the user context by using the transaction ACE_UPDATE the changes are reflected by the ACE runtime tables.

💡 The user context will also be automatically refresh after 16 hours (customizable value)

To maintain user groups you can use the transaction ACE_DESIGN.
To check the authorization data you can use transaction ACE_RUNTIME.

User Data Synchronization

Because ACE references SU01 there is a dependency that requires some attention when you are going to delete a SU01 user.

⚠️ Before deleting a SU01 user, remember the following:

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.
For that use the IMG activities in Customizing under Customer Relationship Management → Basic Functions → Access Control Engine → Rights → Create Rights and under Customer Relationship Management → Basic Functions → Access Control Engine → Update User- and Object Context.

**Authorizations**

This section describes the security-relevant authorization objects that are used by the ACE.

To administrate the ACE design time tables via SM30 or SM34 a user needs the authorization object S_TABU_DIS.

Also following important ACE runtime tables are secured by this authorization object.

- CRM_ACE_ST_ACC
- CRM_ACE_OTYPES
- CRM_ACE_CUSTOM

We recommend not to assign users the S_TABU_DIS authorization for those 3 runtime tables in a productive system.

Furthermore a user needs special authorization to start and to use the ACE transactions ACE_RUNTIME, ACE_UPDATE and ACE_ACTIVATION and to do changes via these tools.

The authorization object CRM_ACE_MD provides the necessary authorization. There exist following values for the field ACTVT:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 (Execute)</td>
<td>A user needs this authorization to start the ACE transactions ACE_ACTIVATION ACE_DESIGN ACE_UPDATE ACE_RUNTIME</td>
</tr>
<tr>
<td>63 (Activate)</td>
<td>A user needs this authorization to activate ACE rights and user groups.</td>
</tr>
<tr>
<td>66 (Refresh)</td>
<td>A user needs this authorization to refresh ACE rights, user- and object-contexts</td>
</tr>
<tr>
<td>H1 (Deactivate)</td>
<td>A user needs this authorization to deactivate ACE rights and user groups.</td>
</tr>
</tbody>
</table>

You should be aware that an user who has these authorization objects assigned has access to all ACE relevant runtime and design data.

**Data Storage Security**

ACE saves runtime and design data in the database of the SAP system, as well as temporarily on the application server(s), e. g. user context cache. The access to the data on the database is restricted by authorization objects.
The runtime data will be written while the activation of rights and after creation / changes of ACE relevant objects by background processes. You can see the status of a right activation by checking the tab Monitoring in transaction ACE_ACTIVATION.

Be aware that failed objects of a right activation means incorrect authorization data. You should correct them by sending them to the update tool using the button 'Send failed objects to update tool'.

During runtime, when authorization queries are made to ACE, the system mainly reads the calculated data. You can check the runtime data by using the transaction ACE_RUNTIME.

Trace and Log Files

You can switch on table logging to log deleting, adding or changing data in the ACE tables e. g. for revision reasons. For each table the audit mechanism logs the user names and the changes that the user makes.

Table logging is enabled for the following database tables in the standard delivery:

- Definition of actor type (CRM_ACE_ACTTYP)
- Customizing (CRM_ACE_CUSTOM)
- Object types (CRM_ACE_OTYPES)
- Rights (CRM_ACE_RIGHTS)
- Rules (CRM_ACE_RULES)
- Assignment of table names to super types (CRM_ACE_ST_ACC)

If necessary, you can also activate logging for the following recommended tables:

- Activated rights (CRM_ACE_RIG_RT)
- Activated user groups (CRM_ACE_UGR_RT)
- Defines determination of actors for the object (CRM_ACE_AFO_CL)
- Defines determination of actors for the user (CRM_ACE_AFU_CL)
- Defines determination of objects via a filter (CRM_ACE_OBF_CL)
- Action groups (CRM_ACE_ANGRP)
- Assignment of actions to action groups (CRM_ACE_ANGRPS)
- User groups (CRM_ACE_U_GRP)
- Assignment of users, roles or groups to user groups (CRM_ACE_U_GRP)
- ACE work package definition (CRM_ACE_WP)
- ACE work package runtime data (CRM_ACE_WP_RT)
- ACE object trace (CRM_ACE_TRACE)

You can activate and deactivate the tables in the ABAP Dictionary. You can view the log results in the table history (transaction SCU3).
Knowledge Management

Introduction

The Knowledge Management (KM) platform of the Enterprise Portal delivers functions and services for managing unstructured- or partially structured content. It enables the user to save and find documents in different types of repository, 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 platform offers generic services, for example, for informing users about changed content and for introducing approval processes into the publishing process. It offers a number of applications that support the collaboration between Portal users, for example, confirmation processes and discussion groups.

CRM Knowledge Management is based on the technology of SAP Portals Knowledge Management. It uses part of the services provided by SAP Portals Knowledge Management. For projects, you can enhance the scope of functions according to the customer’s requirements.

Other Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most important chapter or special restrictions</th>
</tr>
</thead>
</table>

Why do we need Security?

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

Knowledge Management works in a Single-Sign-On environment.


**Authorizations**

**Collaboration Services**

You can restrict collaboration services to role level. This is especially useful for external partners to reduce the access to user data, and/or calendar by other users. For more information refer to Making Services Available [Extern].

**Authorizations for the Info Center directory structure**

You have the option to restrict access to the Info Center according to the 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.

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 the Solution Manager.

**Authorizations for WebDAV Hierarchies**

To publish CRM system documents, set up an http service in the Internet Communication Manager (ICM) of the CRM system. The HTTP service represents the interface of the 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 68676.

For more information on authorizations, see the Solution Manager under Maintaining Authorizations for WebDAV Hierarchies.

**Activating the CRM News Scenario**

If you are using the CRM News Scenario, please be aware that the CRM Namespace Filter is properly configured and is active on your system. If not, it may happen, that an unprivileged user is able to read news, which is not allowed to read.

For more information on the configuration of the news filters, see the Solution Manager under Creating and Adjusting News Filter

Furthermore you have the possibility to restrict access to News Channels (folders in the sapccrmnews repository) by setting Knowledge Management authorizations.

For more information about setting authorizations, see the Solution Manager under Setting Permissions.

**Publish CRM documents via webDAV Handler**

CRM offers the possibility to publish documents which are attached to CRM business objects via a WebDAV server. For more information see the Solution Manager. The documents can be integrated into Portal KM as a webDAV repository, so they can be indexed and searched for with a portal search (TREX).

The corresponding WAS service (/default_host/sap/crm/crm_prt_km_dav) is like all other services deactivated per default. So no documents can reach the outer world.

Activating the service the standard WAS security model holds (For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → SAP Web Application Server Security Guide). The following risks can occur:

- You might enter authentication data into the service or an alias to the service. This of course enables access to anybody and is strongly not recommended. It might be only usefuле for short tests.
Creating a WebDAV repository on portal km side you might enter authentication data into the system landscape entry of the WebDAV repository manager. This again enables anybody who is able to logon to portal to access the CRM documents. This is also not recommended. Instead the landscape option *Same User Domain* should be checked. The user then only sees these documents which he also sees in CRM.
Alerts

Introduction

The following text covers only the area of Alert Management in the portal. It does not cover other security tasks for components that are used or linked to, but which are not part of the Business Productivity Pack.

This chapter applies only for the alert management with the ‘Alert Inbox’ and ‘Alert List’ iView. The following components provide functionality for displaying alerts in the Portal. For further information on the architecture, see the following applications:

- Alert Framework
- SAP CRM 4.0
- Business Package for mySAP CRM - Business Productivity Pack (60.1)
- JCo

Why do we need Security?

Alerts must be protected from unauthorized access, because alerts are connected to activities, which in turn make it possible to view subsequent activities. Viewing an activity can itself also trigger an activity or confirm an alert.

Important SAP Notes

Check regularly for SAP Notes available for application security.

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>703058</td>
<td>Security issue in function modules</td>
<td></td>
</tr>
</tbody>
</table>

System Landscape

The following table describes where you can find additional information about the technical system landscape.

Further information about the system landscape

<table>
<thead>
<tr>
<th>Title</th>
<th>Guide/Tool</th>
<th>Quick Link to the SAP Service Marketplace (service.sap.com)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Management</td>
<td>Alert Management</td>
<td><strong>SAP Help Portal under</strong> help.sap.com → <strong>SAP NetWeaver →</strong> Release '04 → <strong>SAP NetWeaver → Application Platform (SAP Web Application Server) → Business Services → Business Communication</strong></td>
</tr>
<tr>
<td>Services</td>
<td>Alert Management</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td></td>
</tr>
</tbody>
</table>


Roles in the ABAP System for Portal Users

Introduction
The Business Package for SAP CRM 5.0 (60.1) shows content of the following ABAP-systems:

- SAP CRM
- SAP BW
- SAP ERP

If a Portal user wants to use an iView which gets its content from a SAP ABAP system (backend system), he must have a corresponding user in this ABAP system (backend user). Within this system, single and/or corresponding roles (backend roles) are assigned to his backend user. These roles in turn assign authorization objects to the user.

For more information, see the SAP Authorization Concept in the SAP Security Guide.

User Administration and Authentication

User Management
You have to take care that there are corresponding users in the SAP ABAP systems and in the Portal, so that a portal user can access the content from the SAP ABAP systems with his backend user.

For the relation between the name of the user account in the portal and the user name in the SAP ABAP system please see help.sap.com -> Documentation -> SAP Netweaver -> SAP Netweaver Release 04 -> People Integration -> Portal -> Administration Guide -> User Administration -> User Mapping if you are using Single Sign-on or SAP Logon Ticket.

User Data Synchronization
In the portal add all roles to a portal user that are necessary and suitable to his tasks.
In the backend systems add the roles which correspond to the assigned portal roles.

💡 You have to ensure that by adding backend roles you only add those authorizations to a user which he needs to run his portal content. It is important to associate the matching roles to the matching user accounts in the mySAP Enterprise Portal and the SAP ABAP system to ensure correct operation. It might be that there is no corresponding backend role e.g. because the portal role has been changed by adding or deleting content. In this case you have to create your own one which should only contain the authority objects necessary to run the content of the portal role.

⚠️ You must not associate a higher role to the user account in the SAP ABAP system than the portal role associated to the matching portal user (e.g. SAP_PCC_SALES_MANAGER instead of SAP_PCC_SALES_REP). This could allow the portal user (with portal role Sales Representative) to call backend functionality allowed for the role Sales Manager or to see data which is intended for a Sales Manager.

For further information, see Authorizations [Seite 37].
Integration into Single Sign-On Environments

The entire business package is integrated with the SSO environment. We recommend not to use user mapping for the users of the portal roles available in the business package. Most of these portal roles contain iViews based on the following content for which user mapping can restrict integration:

- SAP Business Information Warehouse: For more information, see SAP Help Portal under help.sap.com → SAP NetWeaver → Release ’04 → SAP NetWeaver → Information Integration → SAP Business Information Warehouse → BI Suite: Business Explorer → Integration with the SAP Enterprise Portal

- ISA , Financial Supply Chain Management and Internet Customer Self-Service

CRM Portal KM Extension and DAM need Single Sign-On using SAP logon tickets with user mapping with a SAP Reference System or Single Sign-On using user ID and password with user mapping, also known as Scenario 2 and Scenario 3 in the Portal Security Guide. Only special KM Service user has to be mapped. Please check note 686776 Logon to ABAP engine through KM repository manager.

Authorizations

To access business objects or execute SAP transactions in a backend system, a user requires corresponding authorizations. The authorizations are combined in an authorization profile that is associated with a backend role.

The backend roles and their generated profiles determine what the user is allowed to do within the system. By adding a backend role or a profile to a user, the user receives all authorizations contained in the backend role.

For the portal roles there are corresponding backend roles which allow the use of the content of the Portal role coming from this backend.

If you assign a portal role to a portal user you have to assign the corresponding backend roles to the backend user. You should ensure that the assigned backend roles doesn’t contain more authorities than are necessary for to run the portal content in the assigned portal role.

You can find the list of corresponding roles in the configuration information of the Business Package for CRM in the Solution Manager.

For the content coming from ERP system we do not deliver corresponding backend roles in the ERP system. We do also not ship roles im BW system containing the BW content based on ERP system. You have to create these roles by yourself (see the links below). A description what has to be included in these roles and hints how to create these roles you can find in the configuration information of the Business Package for SAP CRM in Solution Manager.


For automatic creation of corresponding roles in the ABAP system please read: help.sap.com → SAP NetWeaver → Release ’04 → SAP NetWeaver ’04 → SAP Library → SAP NetWeaver → People Integration → Portal → Administration Guide → Content Administration → Roles and Worksets → Portal Roles and ABAP-Based SAP Systems → Role and User Distribution to the SAP System
Checklist

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a portal role there must be corresponding ABAP system roles</td>
<td>The ABAP system user, who corresponds to the portal user, is only assigned to the ABAP roles which correspond to the portal roles which are assigned to the portal user. To find the corresponding roles please see chapter Authorizations.</td>
<td>Use the User Maintenance (transaction SU01) in system to see which roles are assigned to the system user. Logon to the portal with a user assigned to the user administrator role. Navigate to User Administration -&gt; Roles to see which portal roles are assigned to the portal user.</td>
</tr>
</tbody>
</table>
Portal Telephony Integration

The Business Package for SAP CRM 5.0 offers the possibility to call someone directly via the portal application, e. g. in the Accounts Management telephone numbers are shown as link. When you click this link a dialer iView opens. For more information see the Solution Manager under Telephony in the Portal.

Technical System Landscape

The dialer iView communicates with the BCB implementation of the CRM server via a http connection. Target of the connection on the CRM server is the WAS service /default_host/sap/bc/bsp/sap/crm_prt_telctrl which is like all other services deactivated per default.

User Management and Authentication

Integration into the Single Sign-On Environment

Activating this service the standard WAS security model holds. For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → SAP Web Application Server Security Guide. Authentication method is SSO; the dialer iView provides the SSO ticket (cookie) from the portal in its requests to the service.

The following risk might occur (general risk by using WebAS-Services):

We strongly recommend not to enter authentication data into the service or an alias to the service. This of course enables access to anybody; it might be only useful for short tests.

Industry-Specific CRM
Account Origination

Introduction

The financial services business scenario “account origination” is a new application for an integrated customer-oriented software solution, linking the front office (mySAP CRM) to the back office (bank or insurance core processing applications).

Out of the variety of processing flows in the financial services industry, the most prominent and most requested scenario, “loan origination”, was chosen to be realized first.

“Loan origination” is the phase that starts with a customer applying for a loan that is provided by a financial institute, and ends when the contract is signed by both parties. The scenario includes analysis of customer data and requirements, calculation and creation of customer specific offers, underwriting, risk assessment and validation, as well as parts of the closing and funding process.

Related Security Guides

All recommendations concerning mySAP CRM are also relevant for the Account Origination scenario.

In addition the recommendations concerning connected backend systems as the SAP FS-CML, SAP FS-CMS solution and the SAP Credit Managemenet are relevant, see:

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
<th>Most important sections or special restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP CRM</td>
<td>service.sap.com/securityguide</td>
<td>Way to SAP Customer Relationship Management (CRM) Security Guides</td>
</tr>
<tr>
<td>SAP Enterprise Portal</td>
<td>service.sap.com/securityguide</td>
<td>FS-CML, SAP Credit Management, FS-CMS</td>
</tr>
<tr>
<td>SAP Exchange Infrastructure</td>
<td>service.sap.com/securityguide</td>
<td></td>
</tr>
</tbody>
</table>

Authorizations

Account Origination is a cross-system scenario. The linked transactions in Portal concern therefore CRM transactions and backend transaction of i.e. component SAP-CML. The standard SAP authorization concept is in principle sufficient for Account Origination.

In the following section we will provide you with a typical use scenario demonstrating a specific security issue that can arise:

A finance company deals in credits also for employees. The origination process includes also a scoring or rating request whose result will be saved within the business partner and the offer. It must be assured that this data is not visible for other employees in general. This also concerns sensitive data as collaterals, lending values, loans etc.

The security of sensitive data must be ensured. The above described authorization problem could be solved in the following way. Loans for employees, or financial service offers in general for employees, must be created using specific business transaction types and item
types within the CRM One Order. To handle loans for employees an own specific sales organization could be recommended. In addition the user profile of employees should be restricted concerning at least the following authorization objects:

**Authorization Objects**

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_ORD_PR</td>
<td>CRM Order – Business Transaction Type</td>
</tr>
<tr>
<td>CRM_ORD_OE</td>
<td>CRM Order - Allowed Organ. Units</td>
</tr>
</tbody>
</table>

To restrict the FS Account maintenance in CRM concerning specific business partner data in People Centric UI, the user profiles should be restricted concerning at least the following authorization objects:

**Authorization Objects**

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B_BUPA_GRP</td>
<td>Business Partner: Authorization Groups</td>
</tr>
</tbody>
</table>

The People Centric UI for FS Accounts in CRM is based on the People Centric UI for CRM Business Partners and therefore offers the same authorization settings, in particular the authorizations of the Access Control Engine ACE are checked.
SAP Leasing

Introduction

The SAP Leasing solution provides a complete end-to-end solution for all companies that lease out assets. It supports all steps in the financing contract life cycle from a financing opportunity for a lease or a loan to an offer going over to mid-lease changes and resulting in end-of-lease options. Furthermore a remarketing process is combined with the solution for each individual object. The solution also addresses all expected international requirements, including multi-language and multi-currency 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 functionality with world-class CRM capabilities. The complete, end-to-end solution is designed for all financing companies dealing with large volumes of leasing contracts and complex transactions. Therefore the front office (mySAP CRM) is linked seamless with the back office (SAP ERP System).

Related Security Guides

All recommendations concerning mySAP CRM are also relevant for the SAP Leasing scenario. In addition the recommendations concerning connected backend systems as the SAP ERP and SRM are also relevant, see:

### Related Security Guides

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP CRM</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td></td>
<td>→ SAP Customer Relationship Management (CRM) Security Guides</td>
</tr>
<tr>
<td>SAP Enterprise Portal</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td></td>
<td>→ mySAP ERP Security Guides</td>
</tr>
<tr>
<td>SAP Exchange Infrastructure</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td></td>
<td>→ SAP Exchange Infrastructure Security Guides</td>
</tr>
<tr>
<td>SAP Supplier Relationship Management</td>
<td>service.sap.com/securityguide</td>
</tr>
<tr>
<td></td>
<td>→ mySAP Supplier Relationship Management (SRM) Security Guide</td>
</tr>
</tbody>
</table>

Authorizations

Leasing is a cross-system scenario. The linked transactions in Portal concern therefore CRM transactions and backend transaction of i.e. component SAP LAE. The standard SAP authorization concept is in principle sufficient for Leasing.

If the SAP standard authorization concept is not sufficient, customer specific enhancement would be recommended, i.e. using the ACE.

The security of sensitive data must be ensured. This occurs if i.e. employees of your company also occur as business partners leasing a car.

This authorization issue could be solved in the following way. Leasing offers and contracts for employees must be created using specific business transaction types and item types within the CRM One Order. To handle leasing contracts for employees an own specific sales organization could be recommended. In addition the user profile of employees should be restricted concerning at least the following authorization objects:

Authorization Objects
<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_ORD_PR</td>
<td>CRM Order – Business Transaction Type</td>
</tr>
<tr>
<td>CRM_ORD_OE</td>
<td>CRM Order - Allowed Organ. Units</td>
</tr>
</tbody>
</table>

In addition any changes to leasing documents are dependent on the status of the document and the hierarchy level of the user. It is recommended to define a customer-specific structure for leasing document changes within the Customizing under Customer Relationship Management → Financial Services → Leasing and Asset Management → Readiness for Input of Transaction Fields.
Media: Intellectual Property Management (IPM)

Introduction
The SAP for Media Intellectual Property Management (IPM) solution is a comprehensive solution which covers the entire value creation chain for an 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. IPM also contains functions for maintaining business relationships with rights owners, licensors and licensees, actors or authors of Intellectual Property.

Related Security Guides
All recommendations concerning mySAP CRM are also relevant for IPM. In addition the recommendations concerning connected backend system SAP ERP are also relevant, see:

<table>
<thead>
<tr>
<th>Application</th>
<th>Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP CRM</td>
<td><a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a> → SAP Customer Relationship Management (CRM) Security Guides</td>
</tr>
<tr>
<td>SAP ERP</td>
<td><a href="http://service.sap.com/securityguide">service.sap.com/securityguide</a> → mySAP ERP Security Guides</td>
</tr>
</tbody>
</table>

Authorizations
Intellectual Properties are created using a specific product type ('Intellectual Property') in the the CRM product workbench. License contracts are created using specific business transaction types within the CRM One Order. For these specific product types and business transaction types the following authorization objects are provided:

Authorization Objects

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_IPM_AV</td>
<td>IPM Views for Hierarchical Attributes</td>
</tr>
<tr>
<td>CRM_IPMCON</td>
<td>CRM Order Authorization Obj - Bus.Ob. License Usage Confirm</td>
</tr>
<tr>
<td>CRM_IPMGRP</td>
<td>IPM Generation Profiles</td>
</tr>
<tr>
<td>CRM_IPMHIR</td>
<td>IPM Hierarchical Attributes</td>
</tr>
<tr>
<td>CRM_IPMSAC</td>
<td>CRM Order Authorization Obj - Bus.Ob. License Sales</td>
</tr>
</tbody>
</table>
Telco Dealer Application

Other Security-relevant Information

The Telco Dealer application is based on the ICWebClient framework. In contrast to the ICWebClient application itself, it is not used in an intranet environment but in the internet. Therefore all function, pushing information into the application, are disabled.

Checklist

Here you find a checklist with the features, their security settings and how you can prove them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
<th>How to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure secure communication</td>
<td>Is security standard SSL set for ICF Service CRM_IT_DEALER?</td>
<td>You find the activity to activate/ maintain the ICF Services at Customizing under SAP Web Application Server → SAP Web Application Server → Internet Communication Framework → Activate HTTP Services (Tab Logon data)</td>
</tr>
</tbody>
</table>
Master Data
CRM Price List

Introduction
This topic describes the security information for CRM Price List.

Why Is Security Necessary?
Security is necessary, because CRM Price List:

- accesses data in the CRM system, such as business partner information, and consists business data information, such as materials and prices;
- has direct access to the pricing engine where all products and prices are stored and to the tax engine as well;

Therefore, it is very important to restrict access to this data.

User Administration and Authentication

The CRM Price list uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology also apply to the CRM Price list application. For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → SAP Web Application Server Security Guide → SAP Web AS for ABAP Technology.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to the CRM Price List in User Management [Seite 25].

This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the CRM Price list application.

User Management

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

User Management Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and role maintenance with SAP Web AS ABAP (Transactions SU01, PFCG)</td>
<td>For more information, see AP Help Portal help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver 04 → English → SAP Library → SAP NetWeaver → Security → Identity Management → Users and Roles (BC-SEC-USR)</td>
<td></td>
</tr>
</tbody>
</table>

The following users must be created for the CRM Price list:

User Types

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default</th>
<th>Detailed</th>
</tr>
</thead>
</table>

Security Guide for mySAP CRM  670  258
### Password Description

<table>
<thead>
<tr>
<th>User role</th>
<th>Access</th>
<th>User who can</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User who can access Billing transactions. Created by CRM system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>No</td>
<td>System user</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User who can process background jobs</td>
</tr>
</tbody>
</table>

### Authorizations

CRM Price list uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations as described in the SAP Web AS Security Guide ABAP also apply to the application. For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Security Guides for SAP NetWeaver Components → SAP Web Application Server Security Guide.

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

### Standard Roles

The table below shows the standard roles that are used by CRM Price list.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>

### Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by CRM Price list.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEA_PLH</td>
<td>ACTVT</td>
<td>Creation and maintenance of the price list</td>
</tr>
<tr>
<td></td>
<td>APPL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BILL_TYPE</td>
<td></td>
</tr>
</tbody>
</table>
Network and Communication Security

The network topology for CRM Price list 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. For more information see the SAP Help Portal under help.sap.com → Documentation → SAP NetWeaver → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Network and Communication Security and Security Aspects for Connectivity and Interoperability also apply to CRM Price list. Details that specifically apply to the application are described in Communication Channel Security [Seite 40].

This topic describes the communication paths and protocols used by CRM Price list.

Communication Channel Security

Given below are the various communication channels that are used between the components of CRM Price list and other applications:

Communication Paths

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend client using SAP GUI for Windows to mySAP CRM server</td>
<td>DIAG</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to mySAP CRM server</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>Frontend client using a Web browser to SAP Enterprise Portal</td>
<td>HTTP /HTTPS</td>
<td>All application data</td>
<td>Passwords, all sensitive CRM data such as credit card information, customer data, conditions, etc.</td>
</tr>
<tr>
<td>mySAP CRM server to IPC</td>
<td>RFC</td>
<td>Pricing conditions</td>
<td>System information and CRM data</td>
</tr>
<tr>
<td>mySAP CRM server to third-party supplier (TTE or Vertex)</td>
<td>RFC</td>
<td>Tax data</td>
<td>System information and CRM data</td>
</tr>
</tbody>
</table>
Appendix

Related Security Guides
For more information about the security of SAP applications, see SAP Service Marketplace under service.sap.com/security.

You can find the security guides in SAP Service Marketplace under service.sap.com/securityguide.

Related Information
For more information on security-relevant topics, see the links in the table.

Quick Links to related information

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link to the SAP Service Marketplace (service.sap.com)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master guides, installation guides, upgrade guides, solution management guides</td>
<td>instguides</td>
</tr>
<tr>
<td></td>
<td>ibc</td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td>notes</td>
</tr>
<tr>
<td>Released platforms</td>
<td>platforms</td>
</tr>
<tr>
<td>Network Security</td>
<td>network</td>
</tr>
<tr>
<td></td>
<td>securityguide</td>
</tr>
<tr>
<td>Technical infrastructure</td>
<td>ti</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>solutionmanager</td>
</tr>
</tbody>
</table>