SAP Promotion Management for Retail (SAP PMR)

Release 7.0

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

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

Typographic Conventions

Type Style	Description
Example text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.
	Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, F2 or ENTER.

SAP Promotion Management (SAP PMR) Security Guide

Introduction

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

Target Audience

- Technology consultants
- System administrators

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

Why Is Security Necessary?

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

About this Document

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

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**

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

- **Technical System Landscape**

  This section provides an overview of the technical components and communication paths that are used by SAP PMR.

- **User Administration and Authentication**

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

  - Recommended tools to use for user management.
  - Standard users that are delivered with SAP PMR.

  - Overview of the user synchronization strategy, if several components or products are involved.
  - Overview of how integration into Single Sign-On environments is possible.

- **Authorizations**

  This section provides an overview of the authorization concept that applies to SAP PMR.

- **Network and Communication Security**

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

Before You Start

Additional Information

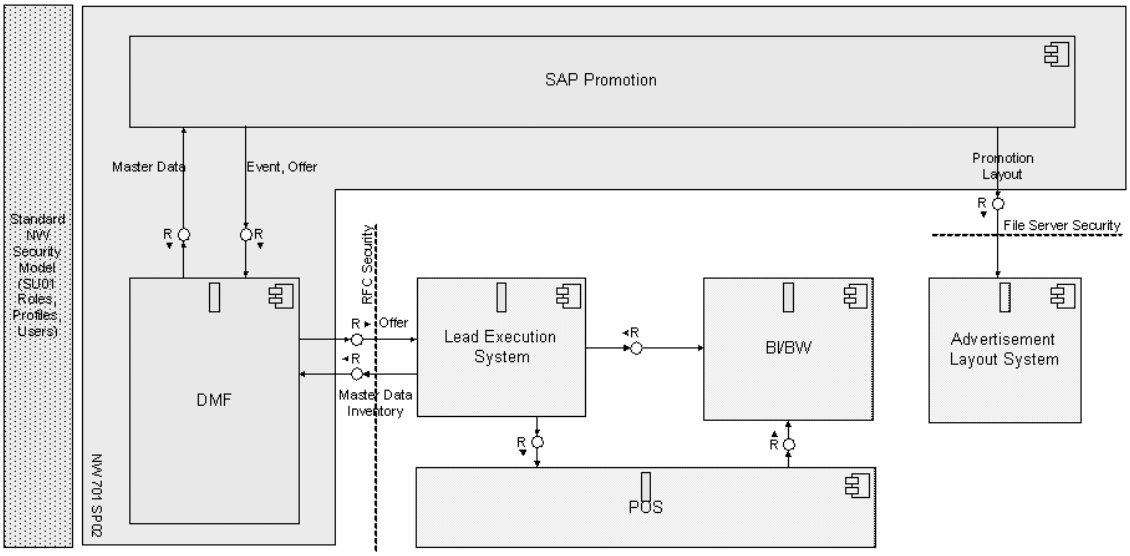
For more information about specific topics, see the addresses on the SAP Service Marketplace as shown in the table below.

Content	SAP Service Marketplace Address
Security	**service.sap.com/security**
Security Guides	**service.sap.com/securityguide**
Related SAP Notes	**service.sap.com/notes**
Released platforms	**service.sap.com/platforms**
Network security	**service.sap.com/securityguide**
SAP Solution Manager	**service.sap.com/solutionmanager**

Technical System Landscape

Use

The figure below shows an overview of the technical system landscape for SAP PMR.



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

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace
Technical description for SAP PMR and the underlying components such as SAP NetWeaver	Master Guide	service.sap.com/instguides
Security		service.sap.com/security

User Administration and Authentication

SAP PMR uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP and Java. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide and SAP NetWeaver Application Server Java Security Guide also apply to SAP PMR. For more information, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guide for Usage Type AS* →

- *SAP NetWeaver Application Server ABAP Security Guide*
- *SAP NetWeaver Application Server Java Security Guide*

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP PMR in the following topics:

- User Management [Page 8]

This topic lists the tools to use for user management and the types of users required with SAP PMR.

- Integration into Single Sign-On Environments [Page 9]

  This topic describes how SAP PMR supports Single Sign-On mechanisms.

User Management

Use

User management for SAP PMR uses the mechanisms provided with the SAP NetWeaver Application Server ABAP and Java, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP PMR, see the sections below.

User Administration Tools

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

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance with SAP NetWeaver AS ABAP (Transactions SU01, PFCG)	For more information, access the following information in http://help.sap.com/: *Technical Operations Manual for SAP NetWeaver → General Administration Tasks → Security and User Administration*	NetWeaver should be running

User Types

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

The user types that are required for SAP PMR include:

- Individual users:
  - Dialog users are used for SAP GUI for Windows or RFC connections.
  - Internet users are used for same policies apply as for dialog users, but used for Internet connections.
- Technical users:
  - Service users are used for authorization to execute promotions.

For more information on these user types, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guide for Usage Type AS* → *SAP NetWeaver Application Server ABAP Security Guide* → *User Authentication* → *User Types*.

Integration into Single Sign-On Environments

Use

SAP PMR supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Security Guide also apply to SAP PMR.

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) in the SAP NetWeaver AS ABAP Security Guide.

SAP logon tickets

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

For more information see, help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guide for Usage Type AS* → *SAP NetWeaver Application Server ABAP Security Guide* → *User Authentication* → *Authentication and Single Sign-On* → *Logon Tickets.*

Client certificates

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

For more information see, help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guide for Usage Type AS* → *SAP NetWeaver Application Server ABAP Security Guide* → *User Authentication* → *Authentication and Single Sign-On* → *Client Certificates.*

Authorizations

Use

SAP Promotion Management uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP apply to SAP PMR.

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

For more information about how to create roles, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *User Administration and Authentication*.

Standard Roles

The table below shows the standard roles that are used by SAP PMR.

Standard Roles

Role	Description
SAP_ISR_PROMO_Marketing	Role that includes access to all Promotions Applications and authorizations (Super User).
SAP_ISR_PROMO_MERCHANDISE	Role that includes access to all Promotions Applications. The Merchandise role has the following authorizations limitation: • Read Only access to Campaign Maintenance (cannot create, edit or delete a Campaign) • Read Only access to Event Maintenance (cannot create, edit or delete an event) Cannot edit or create an offer for which the user is not a member of the owning group • Cannot post or unpost a Template in the Templates application
SAP_ISR_PROMO_ADVERTISING	Role that includes all Promotions Administration Applications and all authorizations for them. The following applications are available for this role: • Templates • Images • Imports • Job Scheduling • Error Recovery
SAP_ISR_PROMO_ADMINISTRATION	Role that all Promotions Administration Applications and limited authorizations for them. The following applications are available for this role: • Templates • Images • Imports • Job Scheduling • Error Recovery The following authorizations are not included: Ability to post or unpost a Template in the Templates application.

Role	Description
SAP_ISR_DMF_MASTER	Role that includes access to only the DMF applications: • Forecast Analytics • Product Groups • Products • Location Hierarchies • Locations • Product / Locations • Transportation Lanes • Job Scheduling • Error Recovery • Imports

Standard Authorization Objects

The security-relevant authorization objects used by SAP Promotion Management are as follows:

CA_POWL: Authorization for Personal Object Work List (POWL) iViews

Object: CA_POWL

Field Name	Value
POWL_APPID	*
POWL_CAT	*
POWL_LSEL	All Values
POWL_QUERY	*
POWL_RA_AL	All Values
POWL_TABLE	All Values

Description: Authorization for POWL Menu functionality for all Promotion POWL Applications. This allows the user to create new powl queries and have all menu options in the powl personal customizing settings.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION
- SAP_ISR_DMF_MASTER

/DMF/CM_AT: Authorization for CM Attribute Assignment

Object: /DMF/CM_AT

Field Name	Value
ACTVT	All Activities

Description: Authorization for user to assign attributes.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/CM_AT: Authorization for CM Image Maintenance

Object: /DMF/CM_IM

Field Name	Value
ACTVT	All Activities

Description: Authorization for Image Maintenance.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION
- SAP_ISR_DMF_MASTER

/DMF/FCANA: Authorization for Forecasting Analytics Execution

Object: /DMF/FCANA

Field Name	Value
ACTVT	All Activities

Description: Authorization for executing Forecasting and Analytics application.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/LANE: Authorization for Lane BO in Consumer Access Layer

Object: /DMF/LANE

Field Name	Value
ACTVT	All Activities

Description: Authorization for access to Transportation Lane Application.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/LOC: Authorization for Location BO in Consumer Access Layer

Object: /DMF/LOC

Field Name	Value
ACTVT	All Activities

Description: Authorization for the access to Location Application.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/LOC: Authorization for Location Hiearchy BO in Consumer Access Layer

Object: /DMF/LOCHR

Field Name	Value
ACTVT	All Activities

Description: Authorization for the access to Location Application.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/PROD: Authorization for Product BO in Consumer Access Layer

Object: /DMF/PROD

Field Name	Value
ACTVT	All Activities

Description: Authorization for the access to Product Application.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/PRDHR: Authorization for Product Hiearchy BO in Consumer Access Layer

Object: /DMF/PRDHR

Field Name	Value
ACTVT	All Activities

Description: Authorization for the access to Product Hierarchy Application.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER

/DMF/dmdts: Authorization for Demand Series in Consumer Access Layer

Object: /DMF/dmdts

Field Name	Value
ACTVT	All Activities

Description: Demand time series is for anyone that needs access to the apis for sales history. This includes any BI interfaces that would be sending POS or consumption data. Authorization for Demand Series in Consumer Access Layer .

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION

/DMF/model: Authorization for Modeling in Consumer Access Layer

Object: /DMF/model

Field Name	Value
ACTVT	All Activities

Description: This is for access to the apis for kicking off modeling (science).

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION

DMF/slsh: Authorization for Sales History BO

Object: /DMF/slsh

Field Name	Value
ACTVT	All Activities

Description: This is for sales history, this again is used for demand time series but the user needs access to read, change, or delete sales history data.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION

DMF/ts: Authorization for Time Series Data in Consumer Access Layer

Object: /DMF/ts

Field Name	Value
ACTVT	All Activities

Description: This is for time series data. Anyone that wants to read, change, or delete time series data (forecast, inventory, modeling, diagnostics, etc) must have this access.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION

/dmf/lbui: Authorization for accessing DMF server config UI

Object: /dmf/lbui

Field Name	Value
ACTVT	All Activities

Description: This is for accessing DMF server config UI.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING

- SAP_ISR_PROMO_ADMINISTRATION

/dmf/opui: Authorization for accessing DMF server config UI

Object: /dmf/opui

Field Name	Value
ACTVT	All Activities

Description: This is for accessing DMF scheduling UI.
Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION

/dmf/inv: Authorization for create and update inventory

Object: /dmf/inv

Field Name	Value
ACTVT	All Activities

Description: This is for create and update inventory.
Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE
- SAP_ISR_DMF_MASTER
- SAP_ISR_PROMO_ADVERTISING
- SAP_ISR_PROMO_ADMINISTRATION

/PRM/CA: Authorization for Coarse Allocation

Object: /PRM/CA

Field Name	Value
ACTVT	'23' 'Maintain'

Description: Authorization to edit mode for the Coarse Allocation application. Those roles that do not include this authorization can only go to the Coarse Allocation application in display only mode.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING

/PRM/CMPN: Authorization for Campaign Maintenance

Object: /PRM/CMPN

Field Name	Value
ACTVT	'23' 'Maintain'

Description: Authorization to create and edit mode for the Campaign application. Those roles that do not include this authorization can only go to the Campaign application in display only mode, cannot create, edit or delete a campaign.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING

/PRM/EVENT: Authorization for Event Maintenance

Object: /PRM/EVENT

Field Name	Value
ACTVT	'23' 'Maintain'

Description: Authorization to create and edit mode for the Event Maintenance application. Those roles that do not include this authorization can only go to the Event application in display only mode, cannot create, edit or delete an Event.

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING

/PRM/OFFR: Authorization for Offer Maintenance

Object: /PRM/OFFR

Field Name	Value
ACTVT	'02' 'Change' '03' 'Display'
/PRM/USGRP	<User Groups in the System>

Description: Authorization to be able to create or edit an offer for the User Group that you belong to. Activity 03, Display, will check to see if the role has access to edit or create Offers for which the user does not belong to the User Group. If this check fails, Activity 02 is checked and the /PRM/USRGRP field is checked to see which User Groups this User has access to create and edit offer for (See User Groups Section for more details).

Included in the following Roles:

- SAP_ISR_PROMO_MARKETING
- SAP_ISR_PROMO_MERCHANDISE

User Groups

SAP Promotion Management will be using an "Owning Groups" concept based on NetWeaver User Groups. Through the Owning Group, the system uses an authority check to determine whether a user has the rights to edit or create an offer.

For example the Merchandise and Marketing roles have different authorities:

- **SAP_ISR_PROMO_Marketing** has access to all Promotion Applications and authorizations
- **SAP_ISR_PROMO_MERCHANDISE** has access to all Promotions Applications with the following authorization limitations:
    - Read Only access to Campaign Maintenance (cannot create, edit or delete a Campaign)
    - Read Only access to Event Maintenance (cannot create, edit or delete an event)
    - Cannot edit or create an offer for which the user is not a member of the owning group
    - Cannot post or unpost a Template in the Templates application

When a user access Offers, the system checks the authorization object /PRM/OFFR. If the user role passes the activity 03 'Display' check, they are able to create and edit Offers from any Owning Group. If the uses role fails the activity 03 'Display' check but passes the 02 'Change' check they can only edit or create offers from Owing Group to which the user belongs.

The general steps to set Owning Groups and authorizations are as follows:

1. Run transaction **SUGR** to create User Groups
2. Assign users to user group
3. Copy one of the delivered template roles to create your implementation specific role
4. Edit the authorization object /PRM/OFFR, Field /PRM/USGRP to set the authorization required in the Promotions-specific role
5. Run transaction **PFCG**
6. Assign the user group to the Promotions role

In this example, we will create an Owning Group for the User Group "Meat":

1. Run transaction **SUGR**
2. Create the user group **Meat**
3. Assign every user you want to be able to edit or create offers in the "Meat owning group" to this user group
4. Copy SAP_ISR_PROMO_Merchandise role to create SAP_ISR_PROMO_Merchandise_Meat
5. Edit authorization object /PRM/OFFR, Field /PRM/USGRP from Value = ***** to Value = **Meat**
6. Run transaction **PFCG**
7. In *Users* tab, assign the Meat User Group to the SAP_ISR_PROMO_Merchandise_Meat role
8. Users access offers in Enterprise Portal would be able to create and edit offers that belong to the **Meat** User Group / Owning Group

A user can belong to multiple User Groups that belong to multiple Merchandising Roles.

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

The network topology for SAP PMR is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to SAP PMR. Details that specifically apply to the SAP PMR are described in the following topics:

- Communication Channel Security [Page 19]

  This topic describes the communication paths and protocols used by SAP PMR.

- Communication Destinations [Page 20]

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

- Network Security

  There are no SAP PMR specific security requirements for this area. SAP PMR follows all SAP NetWeaver standards for network topology, network segments, use of firewalls for access protection, and application ports.

For more information, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide*:

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

Communication Channel Security

Use

The table below shows the communication channel used by SAP PMR, the protocol used for the connection and the type of data transferred.

Communication Channel	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Application server to third-party application	RFC	All application data	none

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

For more information, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Network and Communication Security* → *Transport Layer Security*.

Communication Destinations

If SAP BI is part of your system landscape, SAP PMR requires two RFC destination; one each for BI inbound and BI outbound. The table below provides an overview of the communication destinations used by the SAP PMR 7.0 application. SAP PMR does not include any pre-configured RFC destinations. No other communications destinations other than those listed in the table are required for SAP PMR.

Destination	Delivered	Type	User, Authorizations	Description
Customer Defined in the IMG.	No	RFC	Basis Admin	Inbound from BI: This represents the BI import (delta) load via staging from BI. See Package: `/DMF/BI_INTERFACES_FU` Function Groups: • `/DMF/BI_IF_TS` -- Interface from BI for Time Series • `/DMF/BI_SALES_INBOUND` -- Inbound RFC for BI Sales Data • `/DMF/TS_GENERIC_INBOUND` -- Inbound RFC for Generic Time Series
Customer Defined in the IMG.	No	RFC	Basis Admin	Outbound to BI: This represent the outbound Promotion information sent to BI . The function groups represent data sources that are then used to connect to SAP BI. See Package: `/PRM/EXPORT_BI` Function Groups: • `/PRM/BI_EVENT_EXPORT` • `/PRM/BI_OFR_EXPORT`

Dispensable Functions with Impacts on Security

Use

SAP PMR has no dispensable functions with impacts on security. This section is not applicable for SAP PMR.

Security Logging and Tracing

Use

SAP PMR does not provide additional security logging and tracing above those available within SAP NetWeaver. For more information on:

- Logging and Tracing for ABAP, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Aspects for System Management* → *Auditing and Logging*.
- Logging and Tracing for NetWeaver Business Client, see help.sap.com → *SAP NetWeaver Library* → *Administrator's Guide* → *SAP NetWeaver Security Guide* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guides for Usage Types EPC and EP* → *Portal Security Guide* → *Logging and Tracing* → *Identity Mangement* → *User Management of the Application Server Java* → *Troubleshooting* → *Logging and Tracing*.