Security Guide
Document Version: 1.2 – 2015-02-16

CUSTOMER

SAP Test Data Migration Server

Release 4.0

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	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`	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`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

Version	Date	Change
1.0	2011-08-01	First version of the guide.
1.1	2013-08-08	Authorizations for data scrambling and TDMS BPL Logical paths for data security
1.2	2015-02-16	

Table of Contents

1 Introduction 5

2 Before You Start 7
2.1 Add-On Structure for SAP TDMS 7

3 Technical System Landscape 8

4 User Administration and Authentication 11
4.1 User Data Synchronization 13
4.2 Integration into Single Sign-On Environments 13

5 Authorizations 14
5.1 Standard Authorization Objects 14
5.2 Authorizations at the Activity Group Level 18
5.3 User Roles 25
5.4 Special Considerations 28
5.5 User Registration 28

6 Session Security Protection 29

7 Network and Communication Security 30
7.1 Communication Destinations 31

8 Internet Communication Framework Security 32

9 Application-Specific Virus Scan Profile (ABAP) 33

10 Data Storage Security 34

11 Security-Relevant Logging and Tracing 37

12 Appendix: User Actions Based on the User Role 38

1 Introduction

Caution

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

Target Audience

- Technology consultants
- Security consultants
- System administrators

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

Why Is Security Necessary?

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

These demands on security apply likewise to the SAP Test Data Migration Server (SAP TDMS). Though SAP TDMS is designed for creating non-production systems and is not used for changes to production data, it does deal with data coming directly from production. Also, the use of SAP TDMS involves data transfers from the production system (or a system that is a recent copy of the production system) to the non-production system. Consequently, security issues to be considered in connection with SAP TDMS are, for example, data protection (sensitive data), secure connections between systems, and authorizations. To assist you in securing SAP TDMS, we provide this security guide.

About this Document

The security guide provides an overview of the security-relevant information that applies to SAP TDMS.

Overview of the Main Sections

The security guide comprises the following main sections:

- **Before You Start**

  This section contains 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 TDMS.
- **User Administration and Authentication**

  This section provides an overview of the following user administration and authentication aspects:
  - User types that are required by SAP TDMS
  - User roles that are delivered with SAP TDMS
  - User registration within SAP TDMS
- **Authorizations**

  This section provides an overview of the authorization concept that applies to SAP TDMS.
- **Network and Communication Security**

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

  This section provides an overview of any critical data that is used by SAP TDMS and the security mechanisms that apply.
- **Trace and Log Files**

  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.
- **Appendix**

  This section provides references to further information, including a detailed list of authorizations for the different user roles.

2 Before You Start

Fundamental Security Guides

For a complete list of the available SAP security guides, see the quick link security guide on SAP Service Marketplace. The current version of the SAP NetWeaver security guide, which deals with general security issues, is also available via this quick link.

Additional Information

For more information about specific topics, see the quick links as shown in the table below.

Content	Quick Link on the SAP Service Marketplace
Security	service.sap.com/security
Security Guides	service.sap.com/securityguide
Related SAP Notes	service.sap.com/notes
Related SAP TDMS Notes	Service.sap.com/tdms -> Master Guide for SAP TDMS 4.0
Released platforms	service.sap.com/platforms
Network security	service.sap.com/network service.sap.com/securityguide
Technical infrastructure	service.sap.com/ti
SAP Solution Manager	service.sap.com/solutionmanager

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

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

2.1 Add-On Structure for SAP TDMS

SAP TDMS is available in the following add-ons:

- DMIS: Contains general functions, for example, for the process monitor and for the technical data transfer
- DMIS_CNT: Contains TDMS-specific functions and some of the process types
- This information is important in a security context because the user roles and related settings and functions are included in the add-ons to which they belong from a content perspective (see below for details).

3 Technical System Landscape

Use

The system infrastructure for a data transfer using SAP TDMS requires the following system roles:

- **A sender system** (client) that provides the data supply for the non-production system. The production system is typically used as the sender system. However, there are other options as well.

  For more information, see the solution operations guide for SAP TDMS on SAP Service Marketplace at http://service.sap.com/instguides.
- The **TDMS server**, which includes:
  - A **central system** (client) on which the settings and customizing for the setup of the non-production system are stored. (This central system must be SAP NW 7.0 or higher.)
  - A **control system** (client) from which almost all activities for SAP TDMS are triggered and monitored (This control system must be SAP NW 7.0 or higher.)

    Note

    Any of the systems – except for the receiver system – can be used as the control system. However, we strongly recommend that you implement the TDMS server separately.

  For more information about the types of SAP systems that can be used as the central system and control system for SAP TDMS, see the solution operations guide.
- A **receiver system** (client), which is the non-production system to be filled.
  This may be either a system shell or a full copy of the production system.

Typical Technical System Landscape for SAP TDMS

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

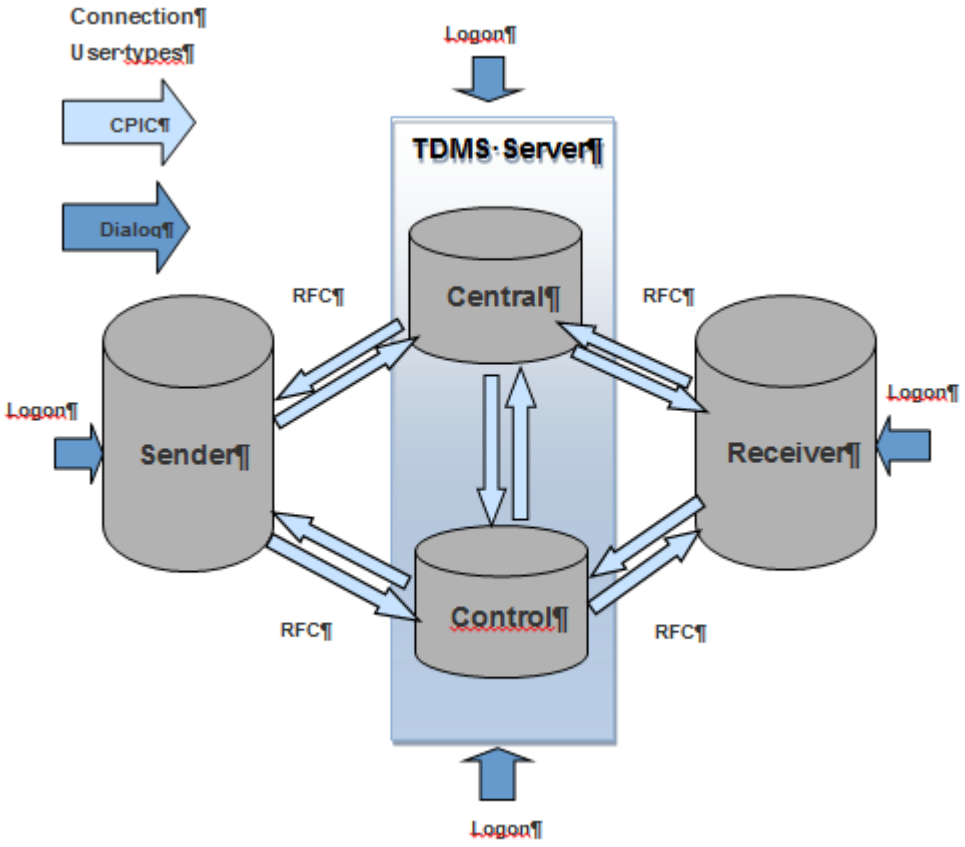

Figure 1: System Landscape for SAP TDMS

To complete the SAP TDMS landscape setup, proceed as follows:

1. Ensure that the system administrator has login access to each of the systems indicated in the figure above.
2. Create login access to the Control system to create a TDMS Project.
3. Create communication users in the Control system.

SAP TDMS automatically creates destinations in the sender, receiver and central systems after the communication users are created in the control system and the landscape is created in the landscape definition manager.

SAP TDMS uses RFC to communicate between different systems. SAP TDMS stores user names, but does not store any passwords. The information stored in the destinations you created using SM59 transaction is used by SAP TDMS.

After you have set up the system landscape and the RFC connections, you can trigger and control all actions (except for a few post-processing tasks) in the different systems through the control system. The control system provides central process control and status management in the process control layer (PCL) of SAP TDMS.

SAP TDMS stores information about all actions (such as status information and log information) in the central system, the control system, and the execution system. SAP TDMS allows you to define the duration of storage for application logs. For more information, see SAP Note 1787871.

Which system should be the central system?

The sender system can also serve as the central system if it is on SAP Basis Release 620 or higher. Any of the systems may be selected as the central system, except for the receiver system. The reason why the receiver

system should not be used as the central system or control system is that the historical data for SAP TDMS needs to be stored permanently, while the receiver system is meant to be refreshed at regular intervals.

Note

In TDMS for HCM projects, if the control system is different from the sender system, you cannot access the sender system using the RFC connection. Rather, the logon screen for the sender system is automatically displayed when the process flow requires you to execute a task in the sender system. For stand-alone scrambling projects, you require a dialog user for the execution system.

Recommendation

We recommend a separate TDMS server to be used as a combined control and central system. Thus it is also possible to control migrations for more than one sender-receiver pair through a single TDMS system.

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

Topic	Guide/Tool	Quick Link on SAP Service Marketplace or SCN
System Landscape	Master Guide for SAP TDMS 4.0	http://service.sap.com/instguides
Security	See applicable documents	See quick link service.sap.com/security

4 User Administration and Authentication

SAP TDMS uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular, the SAP NetWeaver 7.0 Application Server ABAP Security Guide. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver 7.0 Security Guides also apply to SAP TDMS.

This section provides information about user management, administration, and authentication that specifically applies to SAP TDMS in addition to the standard procedures.

Communication User

You require a specific user type called communication user (CPIC) to access different systems using Remote Function Calls (RFC).

- Provide the role `SAP_TDMS_RFC_USER_CR` to the CPIC user where the Basis Release for the remote system is lower than SAP NetWeaver 7.0.
- Provide the role `SAP_TDMS_RFC_USER_700_CR` to the CPIC user where the Basis Release for the remote system is the same as or higher than SAP NetWeaver 7.0.

A communication user can access a system exclusively using RFC and is not allowed to execute steps in dialog mode directly in a system. For more information about this user type, see the section User Types in the SAP NetWeaver 7.0 Application Server ABAP Security Guide.

Security Measures

Carry out the security measures listed below with regard to user management for SAP TDMS:

1. Provide a logon to each system to create the corresponding CPIC users for the administrator of the respective system.
2. Provide a logon to control system to perform the migration steps.
3. Create RFC destinations with passwords for all participating systems in TDMS landscapes.

   Note

   After you create communication users and RFC destinations in the control system, SAP TDMS automatically creates the destinations in the other systems.

- SAP TDMS does not transfer user-related information from the sender system to the receiver system. Therefore, you can separately define the users and authorizations in the receiver system as required. The users and authorizations and are not overwritten during a refresh of the receiver system. Nevertheless, the authorizations in the non-production system should be as similar as possible to those in the production system.
- Regardless of all security measures, users who have access to the control system necessarily have indirect access to the production data in the sender system and may be able to see information stored there.

Recommendation

Since SAP TDMS transfers "productive" data to the non-production system, we recommend that you scramble sensitive data to avoid unauthorized access.

Recommendation

We recommend that you keep the number of users in the control system as small as possible to preclude unauthorized access to production data.

Setup of SAP TDMS Users for Different SAP Frontend Solutions

WebDynpro UI in Browser and NetWeaver Business Client (NWBC)

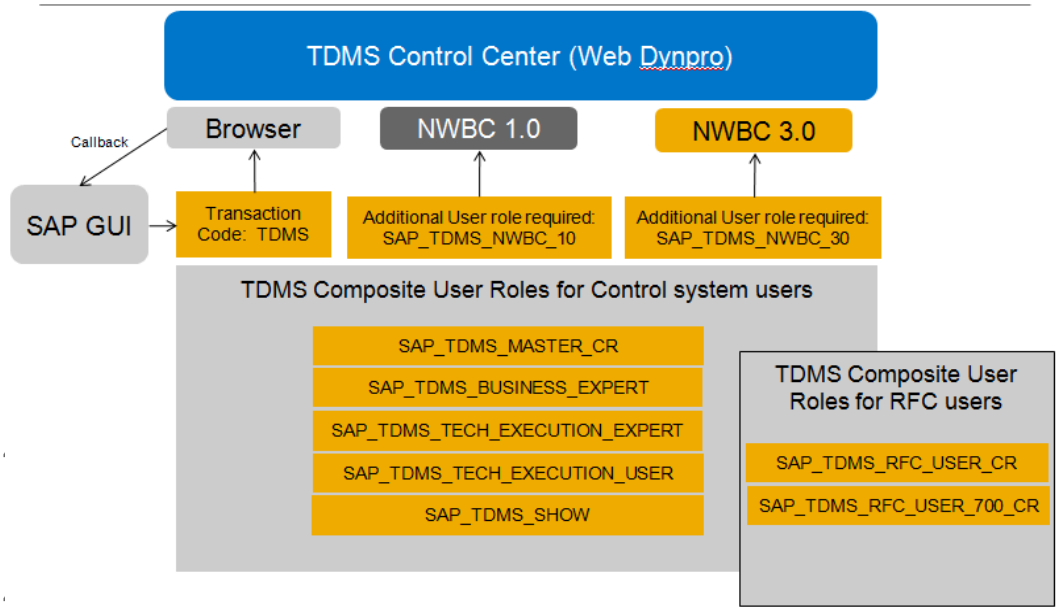

Figure 2: User Roles for Different SAP Frontend Solutions

Recommendation

To run SAP TDMS 4.0, we recommend you use SAP NetWeaver Business Client 3.5 or 4.0. The reason for this is that the SAP NetWeaver Business Client supports a logout for all Web Dynpro windows.

In contrast, web browsers do not support this logout feature. For example, if you use a web browser to access the TDMS work center, there is no option to log out. Simply closing the web browser window does not log the user out of the system. The session runs on the server until it times out, and this is a potential security risk.

User Data Synchronization

Use

User data synchronization (that is, synchronization of user accounts and the associated information, such as passwords) is based on the standard SAP user management synchronization mechanisms. Therefore, the standard recommendations for SAP NetWeaver AS apply to SAP TDMS as well.

For more information, see User Administration and Authentication on SAP Service Marketplace at http://service.sap.com/securityguide ->SAP NetWeaver.

4.3 Integration into Single Sign-On Environments

Use

The SAP TDMS application 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 [SAP Library] also apply to the SAP TDMS application.

The most widely-used 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.

- **SAP logon tickets**

  The SAP TDMS application 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. 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.

- **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.

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

> **Recommendation**
>
> Single Sign-On (SSO) cannot be used for Remote Procedure Calls in SAP TDMS, including in the case of SAP ERP HCM for SAP TDMS, where you are required to manually log in to the sender system.

5 Authorizations

Use

The authorization concept for SAP TDMS builds on standard SAP authorizations. For example, users can only select HCM data for transfer if they have either the standard authorizations for displaying this data or the role `SAP_TDMS_MASTER_CR`.

Recommendation

For information about issues and corrections to user roles and authorizations, see SAP Note 1634482.

Recommendation

You can use the composite role `SAP_TDMS_MASTER_CR` to execute the activities in SAP TDMS. Before you can use `SAP_TDMS_MASTER_CR`, you are required to generate all the single roles defined in the composite role. . You also need to assign authorizations to users using the User Comparison pushbutton to ensure that the users are able to use these composite roles

5.1 Standard Authorization Objects

The following table shows the security-relevant authorization objects that are used by the SAP TDMS application:

Standard Authorization Objects

Relevant Authorization Objects	Fields	Description
S_DMIS Authorization Object for SAP SLO Data Migration Server		
	ACTVT	Activity
	MBT_PR_ARE	MBT PCL: Scenario
	MBT_PR_LEV	MBT PCL: Processing Role Level
S_DMIS_ACT Authorization Object for Activity Group Maintenance		
	`ACTVT`	Activity
	`PROC_TYPE`	MBT PCL Type of Migration Process

Relevant Authorization Objects	Fields	Description
S_DMIS_ADV DMIS Analysis Development Authorization		
	ACTVT	Activity
	MBT_AN_APP	SHC: Analysis Application ID
	MBT_PR_ARE	MBT PCL: Scenario
S_DMIS_AGR Authorization Object for DMIS Activities in Activity Group		
	ACT_GRP	Activity Group
	ACTVT	Activity
	PROC_TYPE	MBT PCL Type of Migration Process
S_DMIS_ANA DMIS Analysis Authorizations		
	ACTVT	Activity
	MBT_AN_APP	SHC: Analysis Application ID
	MBT_PR_ARE	MBT PCL: Scenario
S_DMIS_DEV Development Authority for DMIS		
	ACTVT	Activity
	MBT_PR_ARE	MBT PCL: Scenario
	MBT_PR_NSP	MBT PCL Development Namespace
S_DMIS_PDV DMIS Portfolio Object Development		
	ACTVT	Activity
	MBT_PP_NSP	BTP Object Namespace
	MBT_PP_OBJ	BTP Technical Object Name
	MBT_PP_OTY	BTP Technical Object Type
	MBT_PR_ARE	MBT PCL: Scenario
S_DMIS_PPM DMIS Portfolio and Project Management Authorization		

Relevant Authorization Objects	Fields	Description
	ACTVT	Activity
	MBT_PP_OBJ	BTP Technical Object Name
	MBT_PP_OTY	BTP Technical Object Type
	MBT_PR_ARE	MBT PCL: Scenario
S_DMIS_SCR Authorization Object for Scrambling		
	ACTVT	Activity
	MBT_PR_ARE	MBT PCL: Scenario
	MBT_PR_LEV	MBT PCL: Processing Role Level
TDMS4HCM01 Control for Granular Authority Check		
	TDHC_PA	TDMS4HCM: PA Authorisation Granularity
	TDHC_PD	TDMS4HCM: PD Authorisation Granularity
TDMS4HCM02 TDMS4HCM: Transfer Program Confirm Mode Control		
	TDHC_PACK	Package Number of Transformation / Analysis Package
	TDHC_PROJ	Identification of MBT Project
	TDHC_SPROJ	Identification of MBT Subproject
TDMS4HCM03 TDMS4HCM: Control of Selection of HCM		
	TDHC_SEL	TDMS4HCM: Object Selection - Authorization
S_DMC_S_R MWB: Reading/Writing Authorization in the Sender System/Receiver System		
	ACTVT	Activity
S_DMC_ADMI DMC: Administration Activities		

Relevant Authorization Objects	Fields	Description
	TCD	Transaction Code
	DMC_OBJACT	Activity
	DMC_CNLACT	Activity
	DMC_CUSACT	Activity
	DMC_ADMACT	Activity
S_DMC_COBJ DMC: Conversion Object Activities		
	TCD	Transaction Code
	DMC_OBJACT	Activity
	DMC_CNLACT	Activity
	DMC_CUSACT	Activity
	DMC_ADMACT	Activity
S_DMC_ORGO DMC: Organizational Object Activities		
	DMC_PRJCT	Project IDs
	DMC_SPRJCT	Subproject IDs
	DMC_COBJ	Conversion Object IDs
	TCD	Transaction Code
S_DMC_PRJC DMC: Project Activities		
	TCD	Transaction Code
	DMC_OBJACT	Activity
	DMC_CNLACT	Activity
	DMC_CUSACT	Activity
	DMC_ADMACT	Activity
S_DMC_SPRJ DMC: Subproject Activities		
	TCD	Transaction Code
	DMC_OBJACT	Activity
	DMC_CNLACT	Activity
	DMC_CUSACT	Activity

Relevant Authorization Objects	Fields	Description
	DMC_ADMACT	Activity
S_DMC DMC: Transaction and Activity		
	TCD	Transaction Code
	ACTVT	Activity
	DMC_PRJCT	Project IDs
	DMC_SPRJCT	Subproject IDs
	DMC_COBJ	Conversion Object IDs

Recommendation

Use transaction SU21 to get detailed information on the authorization objects. SAP TDMS uses NetWeaver and application authorizations contained in the roles delivered by SAP TDMS. These authorizations are required for the activities executed by SAP TDMS.

5.2 Authorizations at the Activity Group Level

You may want certain activities to be executable only for certain users or groups of users. For example, you may want to ensure that only users who have certain authorizations are allowed to work with sensitive data. To do so, you can define activity groups (sets of TDMS activities that are related from a content perspective) and assign users or groups of users to these activity groups.

The following **user roles** are relevant in this context:

- Maintain activity groups (SAP_TDMS_ACTGROUP_ADMIN)
- Display activity group definition (SAP_TDMS_ACTGROUP_DISPLAY_USER)
- Role with authorization to execute activities in all activity groups (SAP_TDMS_ACTGROUP_EXEC)

To access the activity group definition, use the transaction CNVMBTACTGRP. On the first screen, you specify the process type that you want to work with. Next, you create the activity groups you need.

To create the corresponding user roles based on role SAP_TDMS_ACTGROUP_EXEC and to assign an activity group to each new role, use the standard role maintenance environment (transaction PFCG).

By default, the activities are not assigned to a particular activity group. Therefore, any user can execute any activity in the process tree.

1. As a first step, create an activity group and assign all the activities in the process tree to this activity group.
2. After the activity group is created, the authorization model becomes operational.
3. Next, assign specific activities of the process tree to the appropriate activity groups.

Note

The activity assignment differs from the authorization concept in the SAP standard.

For more information about assigning activities to activity groups as well as to the appropriate roles and user, see the example below:

Example

1. Create activity groups `TEST_ALL`, `TEST_CUST`, and `TEST_DEF`.
2. Create users `TEST-ALL`, `TEST-CUST`, and `TEST-DEF`.
3. Create and assign roles `ZTDMS_TEST_ALL`, `ZTDMS_TEST_CUST`, and `ZTDMS_TEST_DEF`.
4. Run transaction `CNVMBTACTGRP` and enter the activity group `TEST_ALL`.

   This activity group has the authorization to execute the entire process tree.
5. Assign all the activities to this group. The authorization model becomes operational at this point.

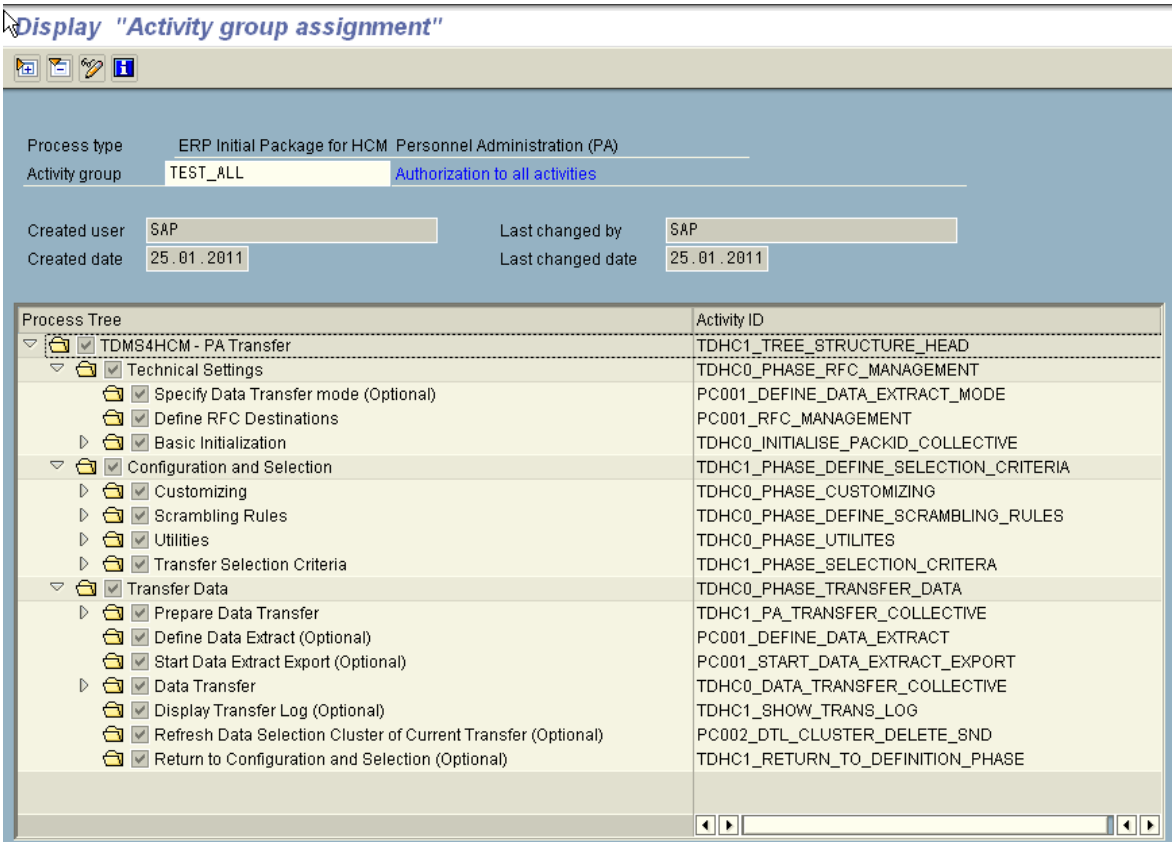

Figure 3: Assignment of Activities to the Activity Group

6. Enter the activity group `TEST_CUST`. This activity group only has the authorization to execute Customizing activities.
7. Assign the respective activities to this group.

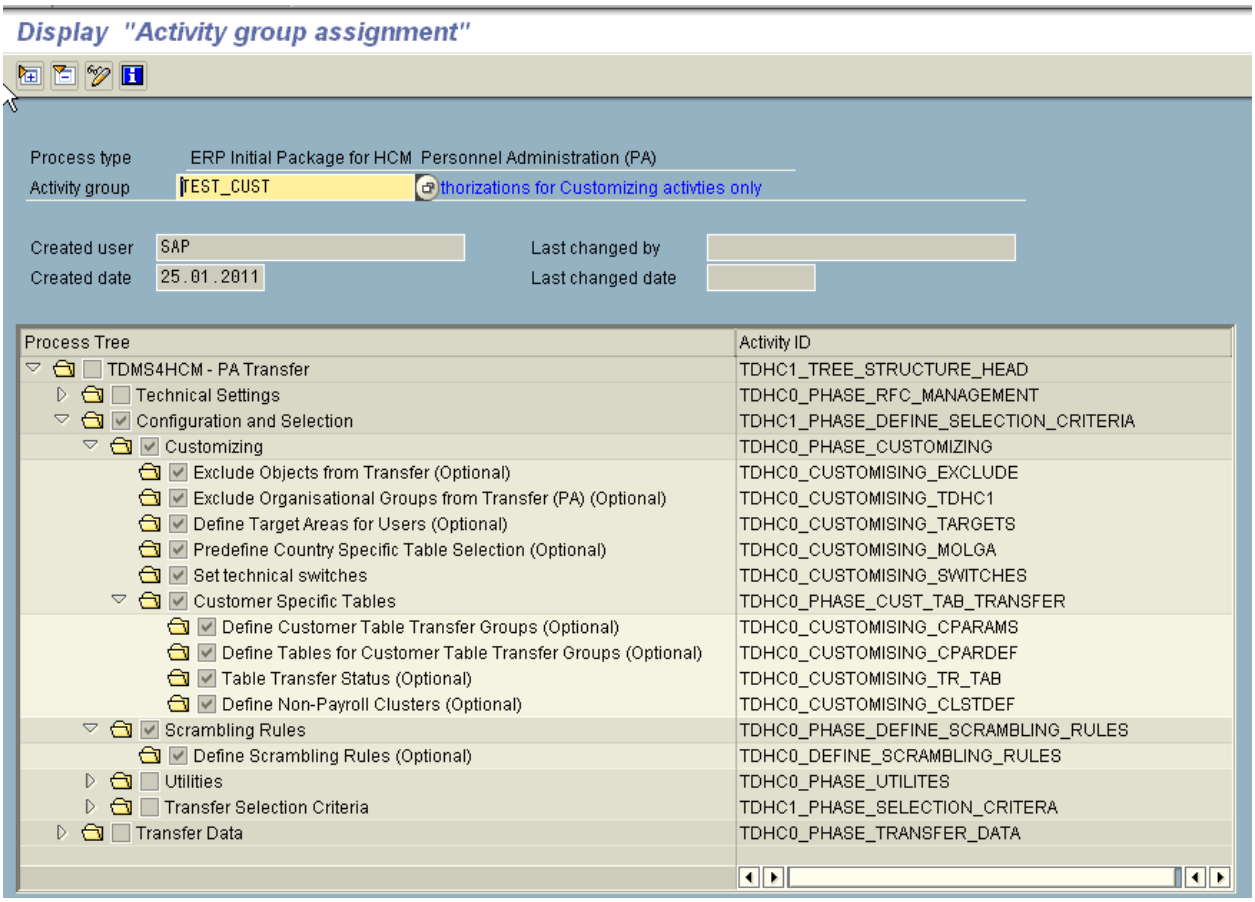

Figure 4: Assignment of Customizing Activities to the Activity Group

8. Enter the activity group `TEST_DEF`. This activity group only has the authorization to execute the data selection and data transfer activities.
9. Assign the respective activities to this group.

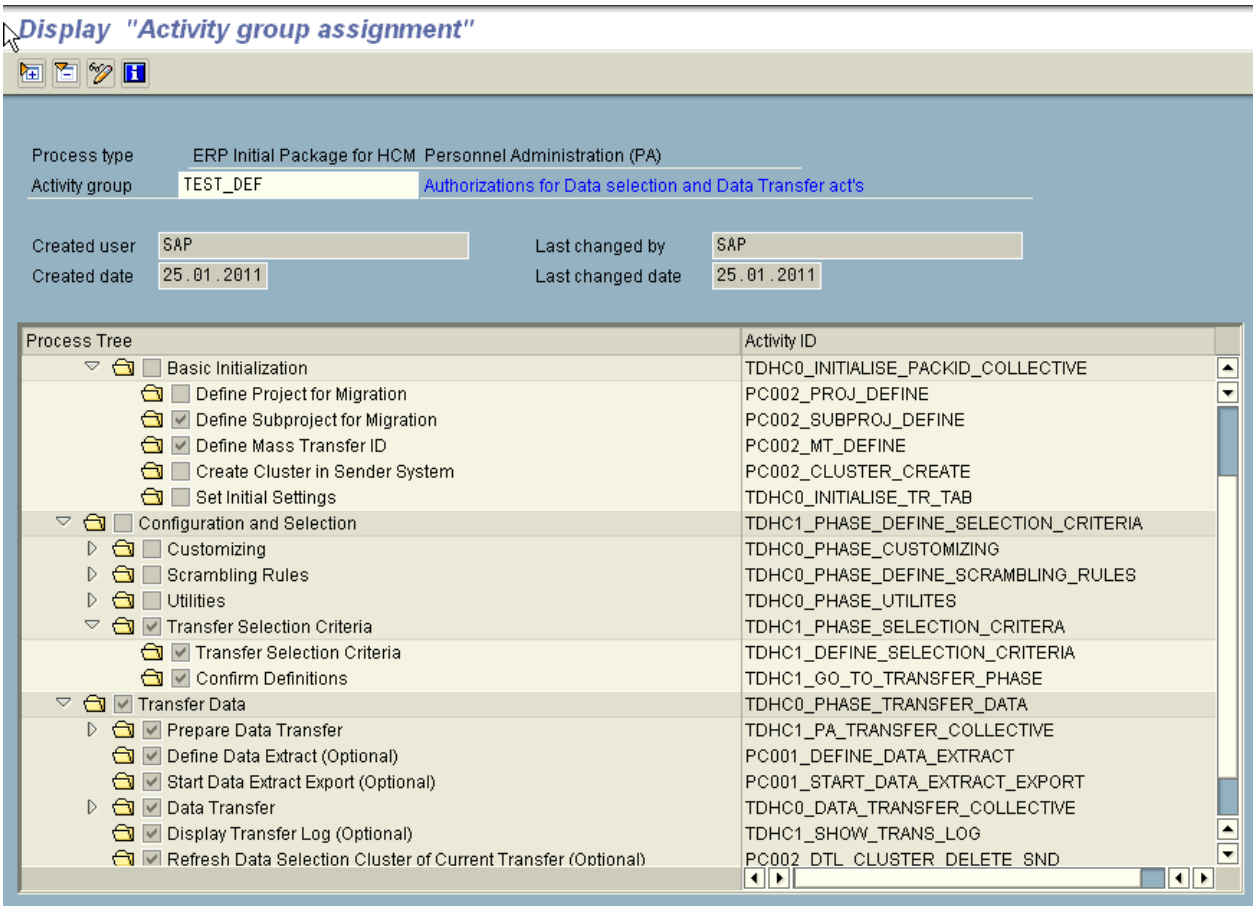

Figure 5: Assignment of Data Selection and Data Transfer Activities

10. Assign the activity groups to the respective roles.

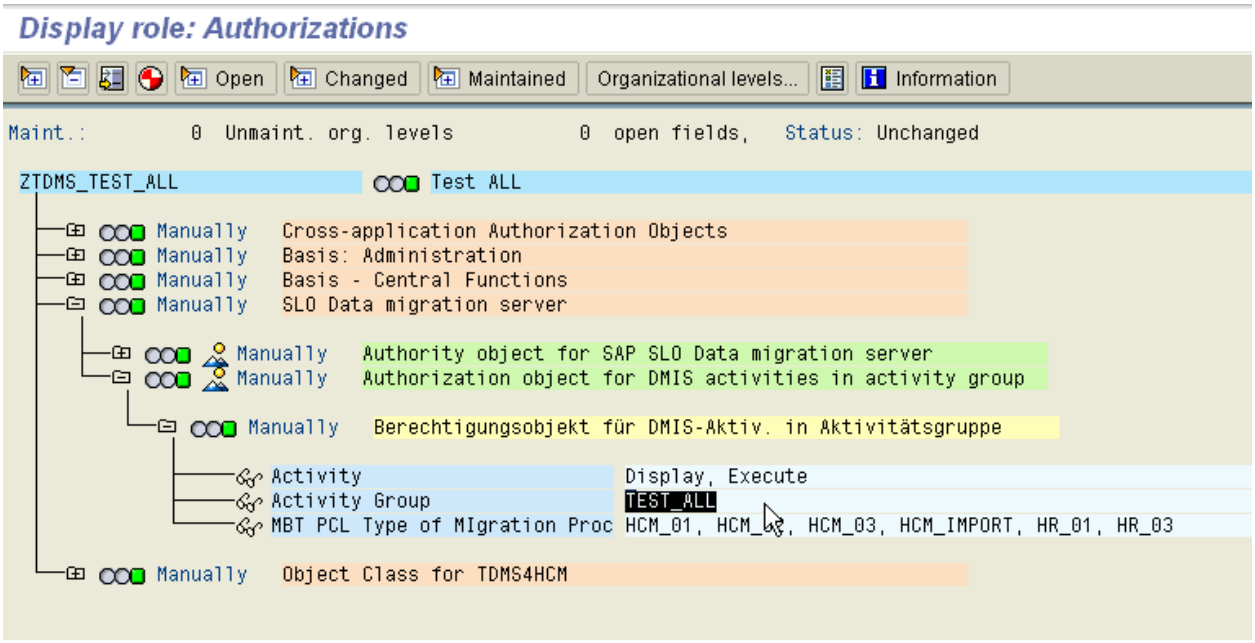

Figure 6: Assignment of Activity Groups to Roles

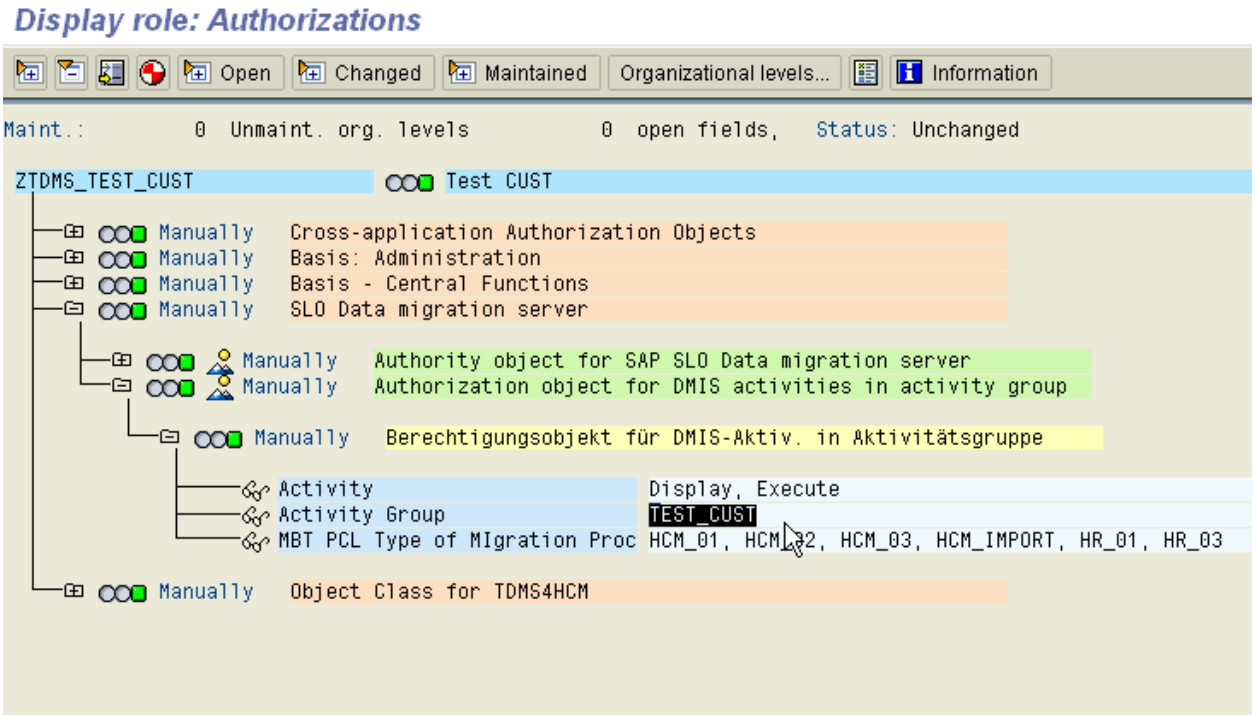

Figure 7: Assignment of Customizing Activity Groups to Roles

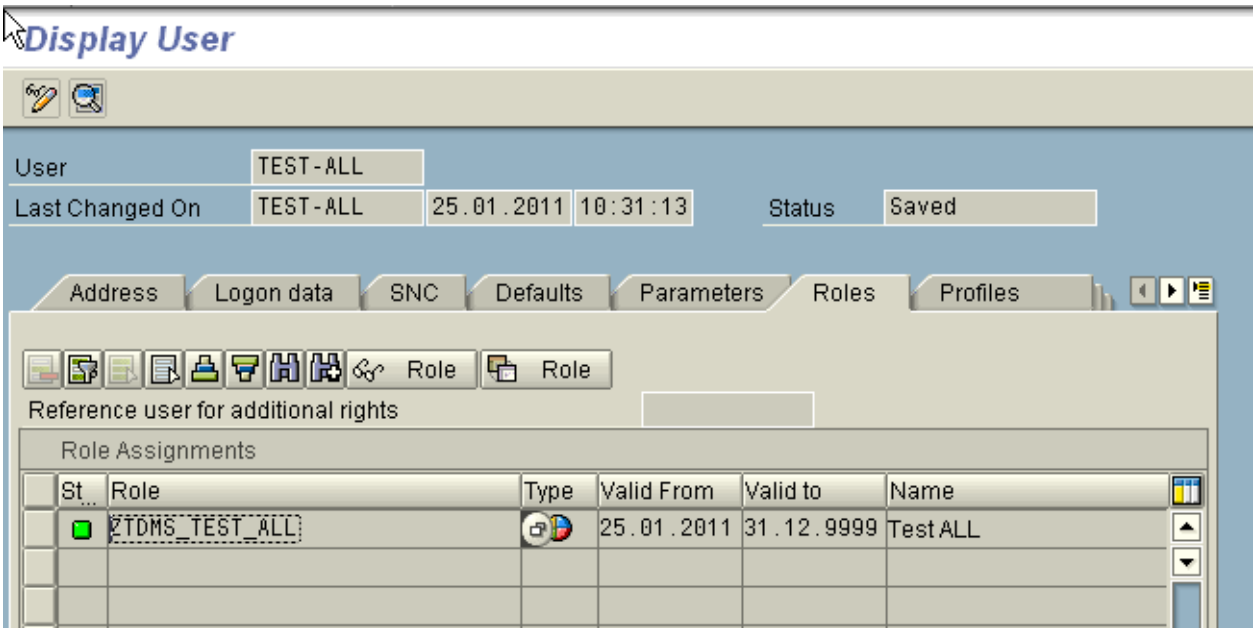

Figure 8: Assignment of Role to the User

11. Assign the roles to respective users.

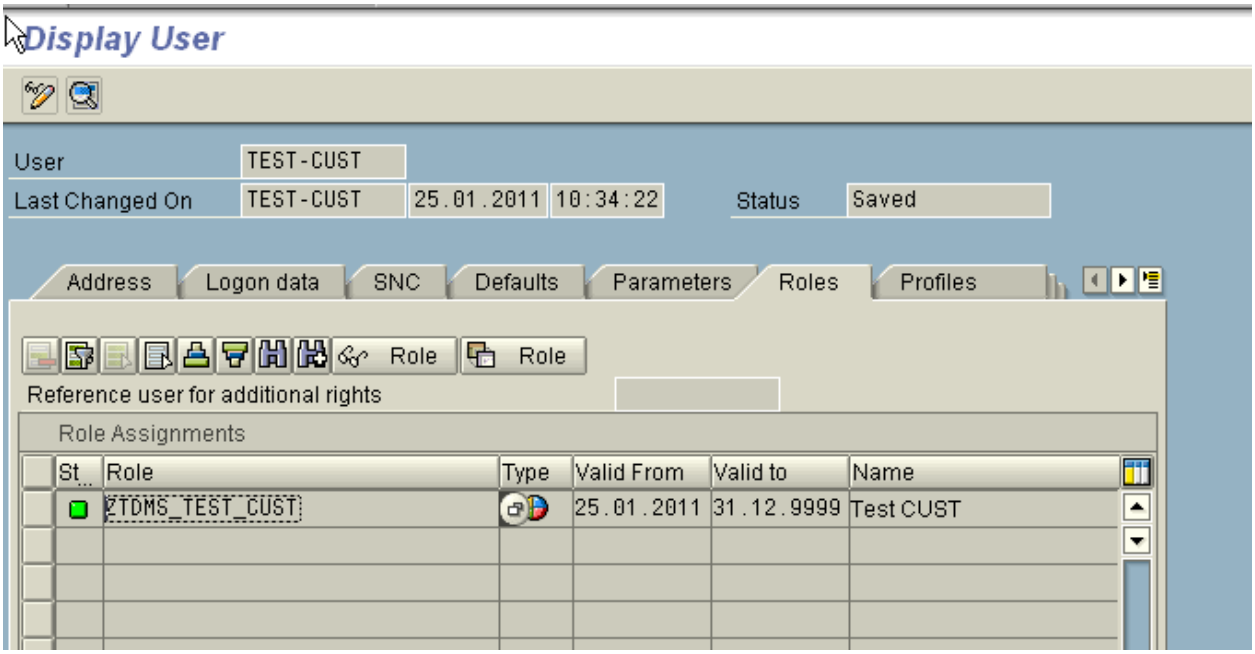

Figure 9: Assignment of Customizing Role to the User

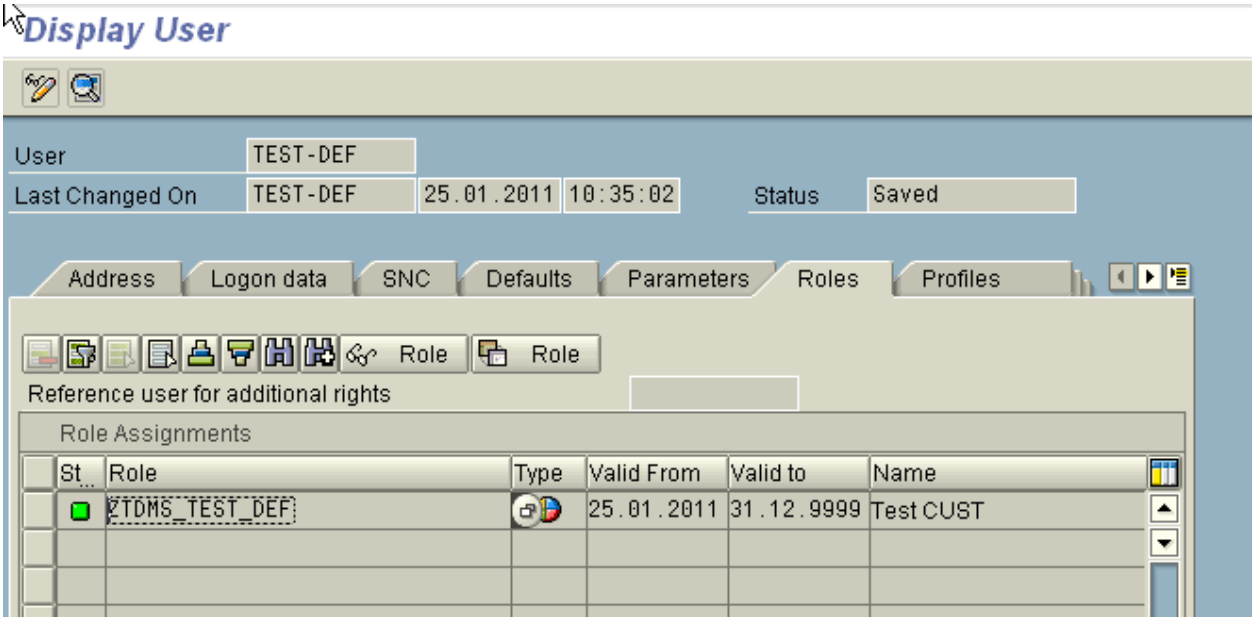

Figure 10: Assignment of Data Selection and Data Transfer Role to the User

5.3 User Roles

From a technical perspective, the following user roles are automatically made available in all systems where the TDMS Add-Ons DMIS and DMIS_CNT are installed:

No.	Role Name	Description
1	SAP_TDMS_MASTER	SAP Test Data Migration Server - Master User (All authorizations)
2	SAP_TDMS_PROJECT_LEAD	SAP Test Data Migration Server - Project Lead
3	SAP_TDMS_USER	SAP Test Data Migration Server - Standard User
4	SAP_TDMS_RFC_USER	SAP Test Data Migration Server - RFC User
5	SAP_TDMS_DISPLAY_USER	SAP Test Data Migration Server - Display User
6	SAP_TDMS_CONTROL_CENTER	SAP TDMS Control Center
7	SAP_TDMS_CONTROL_CENTER_DISPL	SAP TDMS Control Center - Display
8	SAP_TDMS_NWBC_10	SAP TDMS in NWBC 1.0
9	SAP_TDMS_NWBC_30	SAP TDMS in NWBC 3.0
10	SAP_DMIS_TDMS_BASIS	SAP TDMS basis authorizations required in all systems
11	SAP_DMIS_TDMS_BASIS_700	SAP TDMS additional basis authorizations required in all systems from release 700 onwards
12	SAP_DMIS_TDMS_SENDER	SAP TDMS additional basic authorizations required in TDMS sender systems
13	SAP_DMIS_TDMS_RECEIVER	SAP TDMS additional basic authorizations required in TDMS receiver systems
14	SAP_DMIS_TDMS_APPL_1	SAP TDMS additional authorizations 1
15	SAP_DMIS_TDMS_APPL_2	SAP TDMS additional authorizations 2
16	SAP_DMIS_TDMS_APPL_3	SAP TDMS additional authorizations 3
17	SAP_TDMS_HCM_MASTER	SAP TDMS master authorizations required for TDMS HCM
18	SAP_TDMS_HCM_USER	SAP TDMS additional authorizations required for TDMS HCM
19	SAP_TDMS_SCRAMBLING_ADMIN	SAP TDMS Administrator for scrambling settings
20	SAP_TDMS_ACTGROUP_ADMIN	SAP TDMS activity group administrator
21	SAP_TDMS_ACTGROUP_DISPLAY_USER	SAP TDMS activity group display

No.	Role Name	Description
22	SAP_TDMS_ACTGROUP_EXEC	SAP TDMS activity group execution (All groups in all processes)
23	SAP_TDMS_PORTFOLIO_DISPLAY	SAP TDMS Control Center - Portfolio only

In addition, the following composite roles are also available:

Composite Role	Description
SAP_TDMS_MASTER_CR	SAP TDMS Master User - Composite role
SAP_TDMS_BUSINESS_EXPERT	SAP TDMS Business Expert
SAP_TDMS_TECH_EXECUTION_EXPERT	SAP TDMS Technical Execution Expert
SAP_TDMS_TECH_EXECUTION_USER	SAP TDMS Technical Execution User
SAP_TDMS_SHOW	SAP TDMS Display User
SAP_TDMS_RFC_USER_CR	SAP TDMS RFC User for all systems
SAP_TDMS_RFC_USER_700_CR	SAP TDMS RFC User for all systems - Release 700 and higher

Composite Role	Contained Single Roles
SAP_TDMS_MASTER_CR	SAP_TDMS_MASTER
	SAP_TDMS_CONTROL_CENTER
	SAP_DMIS_TDMS_BASIS
	SAP_DMIS_TDMS_BASIS_700
	SAP_DMIS_TDMS_SENDER
	SAP_DMIS_TDMS_RECEIVER
	SAP_TDMS_HCM_USER
	SAP_DMIS_TDMS_APPL1
	SAP_DMIS_TDMS_APPL2
	SAP_DMIS_TDMS_APPL3
	SAP_TDMS_ACTGROUP_ADMIN
	SAP_TDMS_ACTGROUP_DISPLAY_USER
	SAP_TDMS_ACTGROUP_EXEC
	SAP_TDMS_HCM_MASTER
	SAP_TDMS_SCRAMBLING_ADMIN

Composite Role	Contained Single Roles
SAP_TDMS_TECH_EXECUTION_EXPERT	SAP_TDMS_PROJECT_LEAD
	SAP_TDMS_CONTROL_CENTER
	SAP_DMIS_TDMS_BASIS
	SAP_DMIS_TDMS_BASIS_700
	SAP_DMIS_TDMS_APPL1
	SAP_DMIS_TDMS_APPL2
	SAP_DMIS_TDMS_APPL3
	SAP_TDMS_HCM_USER
SAP_TDMS_TECH_EXECUTION_USER	SAP_TDMS_USER
	SAP_TDMS_CONTROL_CENTER_DISPL
	SAP_DMIS_TDMS_BASIS
	SAP_DMIS_TDMS_BASIS_700
	SAP_DMIS_TDMS_APPL1
	SAP_DMIS_TDMS_APPL2
	SAP_DMIS_TDMS_APPL3
	SAP_TDMS_HCM_USER
SAP_TDMS_SHOW	SAP_TDMS_DISPLAY_USER
	SAP_TDMS_CONTROL_CENTER_DISPL
SAP_TDMS_RFC_USER_CR	SAP_TDMS_RFC_USER
	SAP_DMIS_TDMS_BASIS
	SAP_DMIS_TDMS_SENDER
	SAP_DMIS_TDMS_RECEIVER
	SAP_TDMS_HCM_USER
	SAP_DMIS_TDMS_APPL1
	SAP_DMIS_TDMS_APPL2
	SAP_DMIS_TDMS_APPL3
SAP_TDMS_RFC_USER_700_CR	SAP_TDMS_RFC_USER
	SAP_DMIS_TDMS_BASIS
	SAP_DMIS_TDMS_BASIS_700
	SAP_DMIS_TDMS_SENDER
	SAP_DMIS_TDMS_RECEIVER

Composite Role	Contained Single Roles
	SAP_TDMS_HCM_USER
	SAP_DMIS_TDMS_APPL1
	SAP_DMIS_TDMS_APPL2
	SAP_DMIS_TDMS_APPL3

5.4 Special Considerations

SAP TDMS needs the authorization `S_DEVELOP` to generate repository objects (such as programs, data structures) in all affected systems. These objects are required to read the data in the sender system, to scramble the data and export it. Authorization `S_DEVELOP` is used by a batch user only.

We recommend you reduce the authorization of the communication user to limited object namespaces: /CNV/ *, CNV*, /TDM/*, /CMIS/*, /1CADMC/* and DMC* in the sender, central, and receiver systems. The SAP default setting is defined without limitation: namespace (*).

> **Note**
>
> Some of the single roles such as `SAP_DMIS_TDMS_SENDER` do not have authorizations. These roles act as place holders for any new authorizations required for TDMS execution at a later point in time.

5.5 User Registration

In addition to the authorization concept, SAP TDMS has a specific user registration feature. The users need not only the required authorizations for their respective role, but they must also be registered for the projects, and packages they want to work with. This ensures that users can execute functions only in relation to the objects (projects and packages) to which they are assigned.

When you register a user for a SAP TDMS project, the authorizations for executing TDMS are in accordance with the user's technical role.

Registering additional users is the responsibility of the user who created the respective project. The registration at package level also has to be done for users in remote systems.

SAP TDMS also offers functions for locking all non-registered users before the start of the actual data transfer in a migration and for unlocking them again afterwards. This is an additional precaution against actions in the system that might interfere with the data transfer. You can also register the users of the receiver system to ensure that these users are not locked during data transfer.

Users specified in RFC destinations are automatically registered in the corresponding system so that they are not locked during the data transfer.

6 Session Security Protection

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

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

Session Security Protection on the AS ABAP

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

For more information, a list of the relevant profile parameters, and detailed instructions, see Activating HTTP Security Session Management on AS ABAP [SAP Library] in the AS ABAP security documentation.

7 Network and Communication Security

Access to all sender systems and receiver systems in an SAP TDMS system landscape takes place exclusively through RFC connections as the communication channel. SAP TDMS does not provide any encryption for this communication channel. SAP TDMS does not use any ports apart from the ones used for WebDynpro, which comply with the security standards for SAP NetWeaver.

The SNC (Secure Network Communication) component provides enhanced security by encrypting data and ensuring more secure authentication by both systems in a communication. You can enable this component, by choosing your RFC connection in transaction SM59 and choosing the *Logon and Security* tab page. We recommend that you enable Secure Network Communication for your RFC connections. For more information, see the RFC/ICF Security Guide on the SAP Help Portal at http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/92486caa6b17cee10000000a421937/frameset.htm.

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 level 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 TDMS 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 TDMS.

Details that specifically apply to SAP TDMS are described in the following topic:

- Communication Destinations

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

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

  and Communication Security [SAP Library]

- Security Guides for Connectivity and Interoperability Technologies [SAP Library]

7.1 Communication Destinations

Use

TDMS does not come with fixed destinations or user names. The Landscape Definition Manager takes care of distributing the destinations to all participating systems.

You must create the following destinations:

- Connect the control and central system by RFC to all participating systems. Each system must also have a destination directed to itself.
- Connect the sender system and the receiver system to the control system and to the central system. Ensure that each system also has a destination directed to itself.

If the destinations are distributed and synchronized using the RFC management provided by SAP TDMS, the destinations described above are created automatically.

The following general security measures regarding RFC and related issues have been taken:

- Any change of an RFC destination used for a migration is detected to avoid the execution of steps in the wrong system.
- The history of destination configuration changes is stored so as to keep the information about previous migration projects.
- Authorizations of CPIC and logon users are restricted to the minimum needed for performing the required actions in the relevant systems. The CPIC users need all authorizations defined in the user role `SAP_TDMS_USER`.
- RFC destinations can be deleted or invalidated after completion of the migration, as information about the migration will be available in the control system.

For more information about RFC management for SAP TDMS, see the related online activity documentation.

8 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For *SAP TDMS* the following services are needed in the control system:

- *CNV**
- *BTP**

Use the transaction SICF to activate these services.

If your firewall uses URL filtering, note the URLs used for the services and adjust your firewall settings accordingly.

For more information, see Activating and Deactivating ICF Services [SAP Library] in the SAP NetWeaver Library documentation.

For more information about ICF security, see the RFC/ICF Security Guide [SAP Library].

9 Application-Specific Virus Scan Profile (ABAP)

SAP provides an interface for virus scanners to prevent manipulated or malicious files from damaging the system. To manage the interface and what file types are checked or blocked, there are virus scan profiles. Different applications rely on default profiles or application-specific profiles.

To use a virus scanner with the SAP system, you must activate and set up the virus scan interface. During this process, you also set up the default behavior. SAP also provides default profiles.

For more information, see SAP Virus Scan Interface [SAP Library] and SAP Note 1693981 *(Unauthorized modification of displayed content)*.

10 Data Storage Security

Use

SAP TDMS does not create or store any sensitive data even temporarily in the control or central systems. However, during data selection, SAP TDMS extracts data relevant for migration from the application tables of the sender system and stores it separately in a cluster format. If any data scrambling rules are active, then these rules are applied on the cluster data, which is later transferred to the receiver system.

This data is not accessible to the SAP TDMS dialog user. However, the data protection depends on the sender system being marked as a production client, or by restricting access to table RSINDX00, which has administrative authorizations.

You can access the data stored in the SAP TDMS data cluster with the transaction DTLMON. On entering the transaction, you must specify the mass transfer ID and the access plan for the current package. A new screen is rendered, on which you can access the information of data volume for every migration object (Runtime Information tab).

By default, SAP TDMS copies data as it is from the sender system to the receiver system depending upon the portfolio item selected. Some portfolio items like Client Based Transfer facilitate the transfer of the data of the entire client, except when specifically excluded. Other portfolio items like Business Process Library transfer the data specific to the selected business process. You can find more information about the available portfolio items in Section 3 of the SAP TDMS Master Guide. If you do not want some specific sensitive data to be transferred, SAP TDMS can give a scrambling framework to anonymize this data before it is transferred to the non-productive environment.

You can transfer data in SAP TDMS using one of the following methods:

- Direct transfer between systems through RFC.
- Transfer using RFCs allows for a high level of security.
- Data transfer through file export and import

Data Transfer Through Files

- Data transfer through files allows you to create an optimal throughput and allows you the flexibility of creating multiple imports with the same export file.
- When you carry out a file export, SAP TDMS creates a binary data file containing the database records of the cluster table. The cluster table stores the data to be transferred to the receiver system.
- SAP TDMS does not encrypt the exported file.
- To import the file into a receiver system, you must have the relevant SAP TDMS authorizations.
- The import populates data into the SAP TDMS cluster table in the receiver system.
- To load the relevant application tables from the cluster table, execute the appropriate process tree for the Data Import Through Files migration solution.

> **Note**
>
> To export the files, you can use the transport directory or any other folder that has the appropriate access restrictions.

Deletion of Temporarily Stored Data

SAP TDMS allows you to delete all the temporarily stored data once the data transfer is complete. You can do this by executing the activity Refresh of Data Selection Cluster in the current transfer in the post-processing phase.

Data Flow Diagram

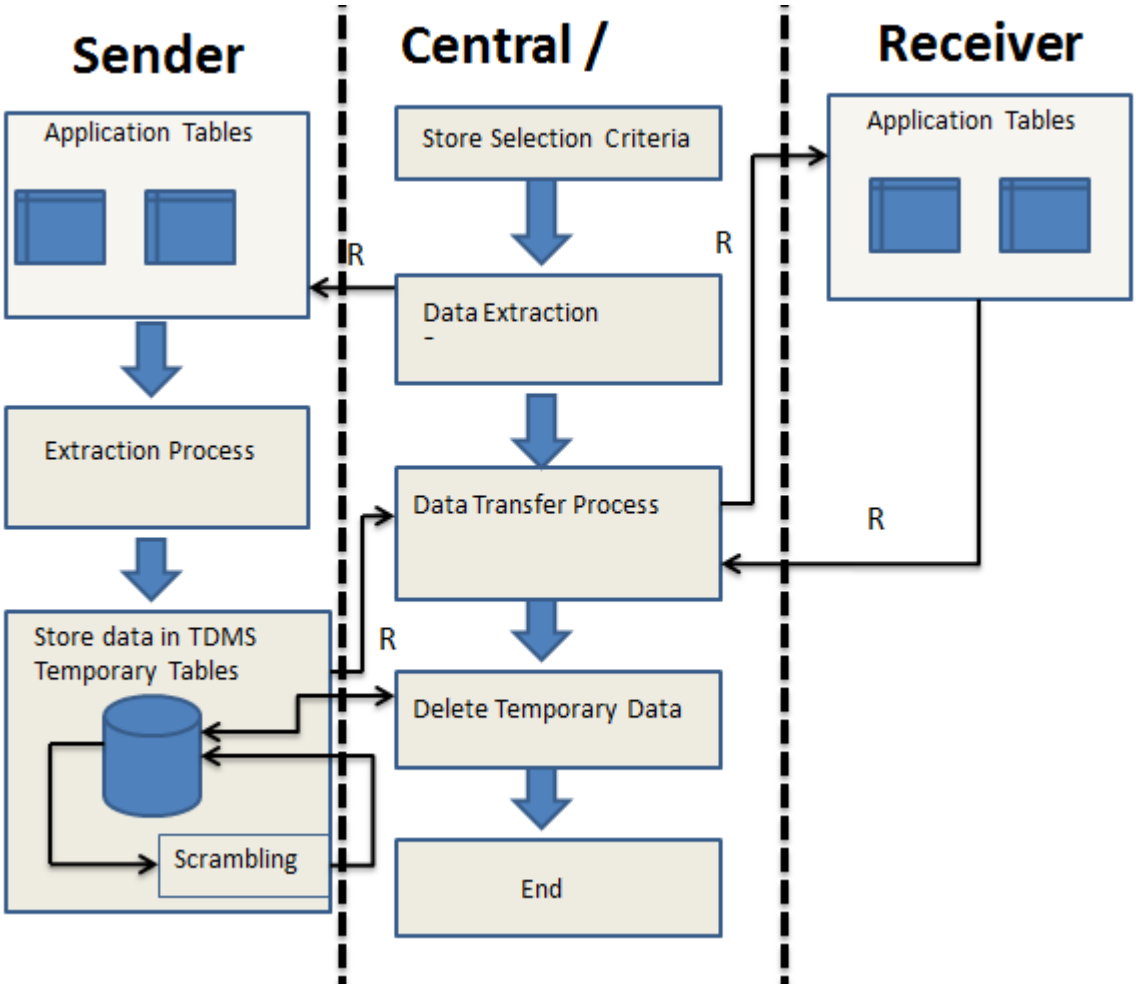

Figure 11 Data Flow Diagram for SAP TDMS

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

SAP TDMS saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as path

traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory (including subdirectories) that does not match a stored mapping, then an error occurs.

The following lists show the logical paths used by SAP TDMS and for which programs these file names and paths apply:

Logical Path Names Used in SAP TDMS

The logical file names listed above all use the logical file path *DMIS_DEX_ROOT.*

Activating the Validation of Logical Path and File Names

These logical paths, as well as any subdirectories, are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client-independent). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see:

- Logical File Names [SAP Library]
- Protecting Access to the File System [SAP Library]
- Security Audit Log [SAP Library]

11 Security-Relevant Logging and Tracing

Use

SAP TDMS does not create any trace files. However, SAP TDMS writes log files (application log) for each activity in the migration process tree. These logs show which user executed a given activity at what time and for which systems.

You can access the log files from the procedure monitor for SAP TDMS.

12 Appendix: User Actions Based on the User Role

Note

This list only covers the roles that come with add-on DMIS_CNT.

		SAP_TDMS_PORTFOLIO_DISPLAY(*)	SAP_TDMS_SHOW	SAP_TDMS_BUSINESS_EXPERT	SAP_TDMS_TECH_EXECUTION_USER	SAP_TDMS_TECH_EXECUTION_EXPERT	SAP_TDMS_MASTER_CR	SAP_TDMS_RFC_USER_700_CR	SAP_TDMS_RFC_USER_CR
Control System Authorizations TDMS Control Center									
Area	Action								
Overview	Display Overview screen	X	X	X	X	X	X	-	-
Portfolio	Display / Navigate in Portfolio	X	X	x	X	X	X	-	-
Project Templates	Display Project Template overview	-	X	X	X	X	X	-	-
	Display Project Tempate	-	X	X	X	X	X	-	-
	Create Project Template	-	-	X	-	X	X	-	-
	Edit foreign Project Template	-	-	-	-	-	X	-	-
	Edit own Project Template	-	-	X	-	X	X	-	-
	Delete foreign Project Template	-	-	-	-	-	X	-	-
	Delete own Project Template	-	-	X	-	X	X	-	-
Projects	Display list of Projects	-	X	X	X	X	X	-	-
	Display details of foreign Project	-	X	X	X	X	X	-	-
	Display details of own/assiged Project	-	X	X	X	X	X	-	-
	Edit foreign Project	-	-	-	-	-	X	-	-
	Edit own/assigned Project	-	-	X	-	X	X	-	-
	Delete foreign Project	-	-	-	-	-	X	-	-
	Delete own/assigned Project	-	-	X	-	X	X	-	-
	Create Project	-	-	-	-	X	X	-	-
	Compose foreign Project	-	-	-	-	-	X	-	-
	First Composing of own / asssigned project	-	-	X	-	X	X	-	-
	Compose own/assigned Project	-	-	X	-	X	X	-	-
	Extend foreign Project	-	-	-	-	-	X	-	-
	Extend own/assigned Project	-	-	X	-	X	X	-	-
	Create TDMS Transfer package	-	-	-	-	X	X	-	-
	Execute TDMS Transfer package	-	-	-	X	X	X	-	-
	Display TDMS Transfer package	-	X	X	X	X	X	-	-

Remote System Authorizations

Remote System authorizations (RFC User)	-	-	-	-	-	X	-	-
Execute TDMS actions in Remote System (<700)	-	-	-	-	-	X	-	X
Execute TDMS actions in Remote System (>=700)	-	-	X	X	X	X	X	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-

Scrambling Authorizations

Area	Action	SAP_TDMS_PORTFOLIO_DISPLAY (*)	SAP_TDMS_SHOW	SAP_TDMS_BUSINESS_EXPERT	SAP_TDMS_TECH_EXECUTION_USER	SAP_TDMS_TECH_EXECUTION_EXPERT	SAP_TDMS_MASTER_CR
Scrambling	Open the workbench and view	-	-	X	-	-	X
	View the rules in the workbench	-	-	X	-	-	X
	Edit the rules in the workbench	-	-	X	-	-	X
	Create the rules in the workbench	-	-	X	-	-	X
	Copy the scrambling content to the Project	-	-	X	-	X	X
	View the rules from the project	-	-	X	-	-	X
	Select the rules in the Project	-	-	X	-	X	X
	Edit the rules from the project	-	-	X	-	-	X
	Create the rules in the project	-	-	X	-	-	X
	Execute the scrambling activity	-	-	-	X	X	X

	Copy the scrambling content to the Package	-	-	-	X	X	X
	View the rules from the package	-	-	-	-	-	X
	Select the rules in the Package	-	-	-	X	X	X
	Edit the rules from the package	-	-	-	-	-	X
	Create the rules in the package	-	-	-	-	-	X

BPL Authorizations

Area	Action	SAP_TDMS_SHOW	SAP_TDMS_BUSINESS_EXPERT	SAP_TDMS_TECH_EXECUTION_EXPERT	SAP_TDMS_TECH_EXECUTION_USER	SAP_TDMS_MASTER_CR
BPL	Display BPL Overview screen	X	X	X	X	X
	Display/Navigate to BPL object details screen	X	X	X	X	X
	Create custom BPL objects	-	X	X	-	X
	Copy BPL objects	-	X	X	-	X
	Edit custom BPL objects	-	X	X	-	X
	Create Variant for BPL Packages	-	X	X	-	X
	Validate Variant for BPL Packages	-	X	X	-	X
			S_DMIS with create and change authorization in Remote system	S_DMIS with create and change authorization in remote system	-	S_DMIS with create and change authorization in remote system

www.sap.com/contactsap