Security Guide for SAP Test Data Migration Server (SAP TDMS)

HELP.NWSECGUIDE

Version 2.5

February 2011

Copyright

Icons in Body Text

Icon	Meaning
⚠	Caution
💬	Example
💡	Note
🧭	Recommendation
SYN	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`.

Introduction

⚠

This guide does not replace the daily operations handbook that we recommend customers should create for their specific day-to-day operations.

Target Audience

- Consultants
- Security specialists
- (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 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 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 bySAP 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, in particular a detailed list of authorizations for the different user roles.

Before You Start

Fundamental Security Guides

Fundamental Security Guides

For a complete list of the available SAP security guides, see the quick link securityguide 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.

Quick Links to Additional Information

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
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

Add-On Structure for SAP TDMS

SAP TDMS is shipped 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
- DMIS_EXT: For various process types; currently, it contains only the process type for business process library
- DMIS_BSC: For the process types to be used with SAP BI or CRM systems
- DMIS_HR: For the process types to be used in the context of SAP Human Capital Management (HCM)

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).

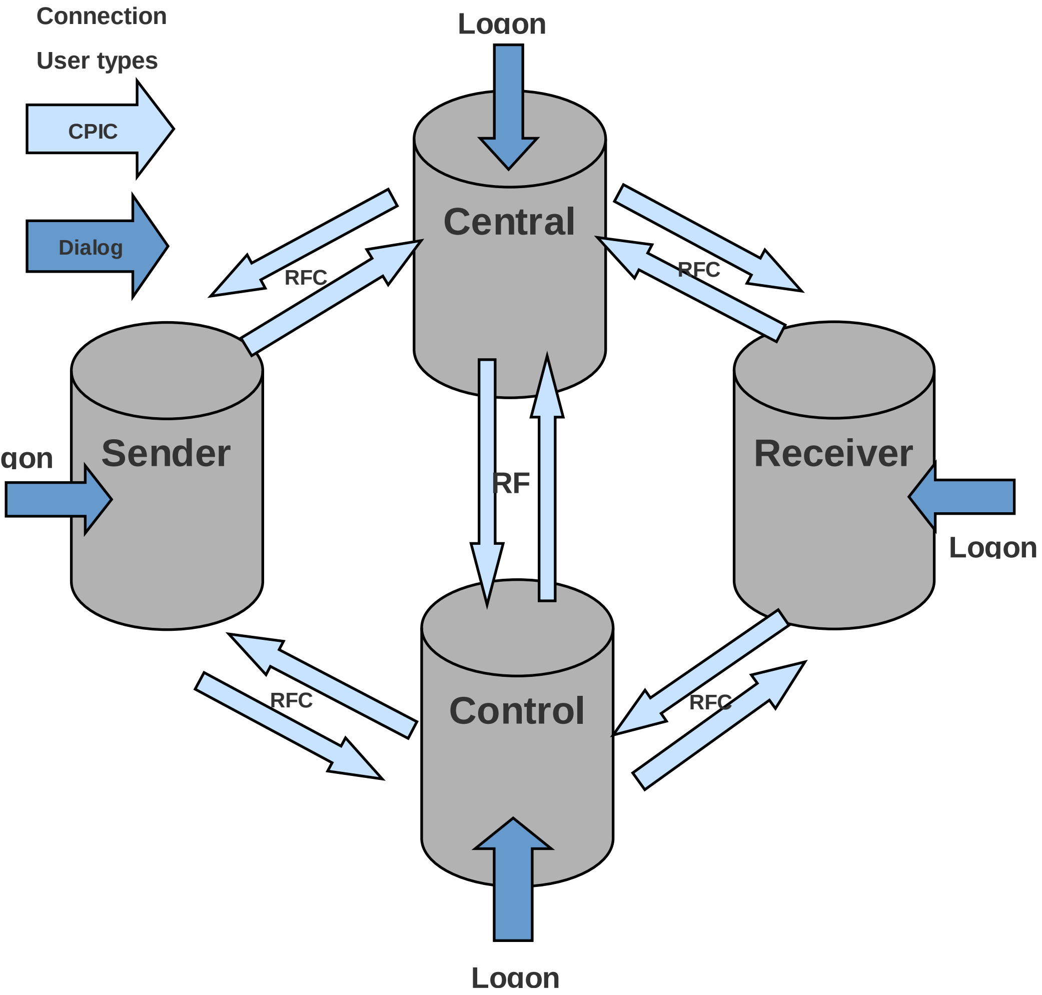
Technical System Landscape

SAP TDMS runs on a system infrastructure that contains

- A sender system (client) with productive data (may be a copy or mirror)
- A central system (client) (at least WAS 620)
- A control system (client)
- A receiver system (client) (the non-production system to be filled)´

The central system and the control system are jointly referred to as the **TDMS server**.

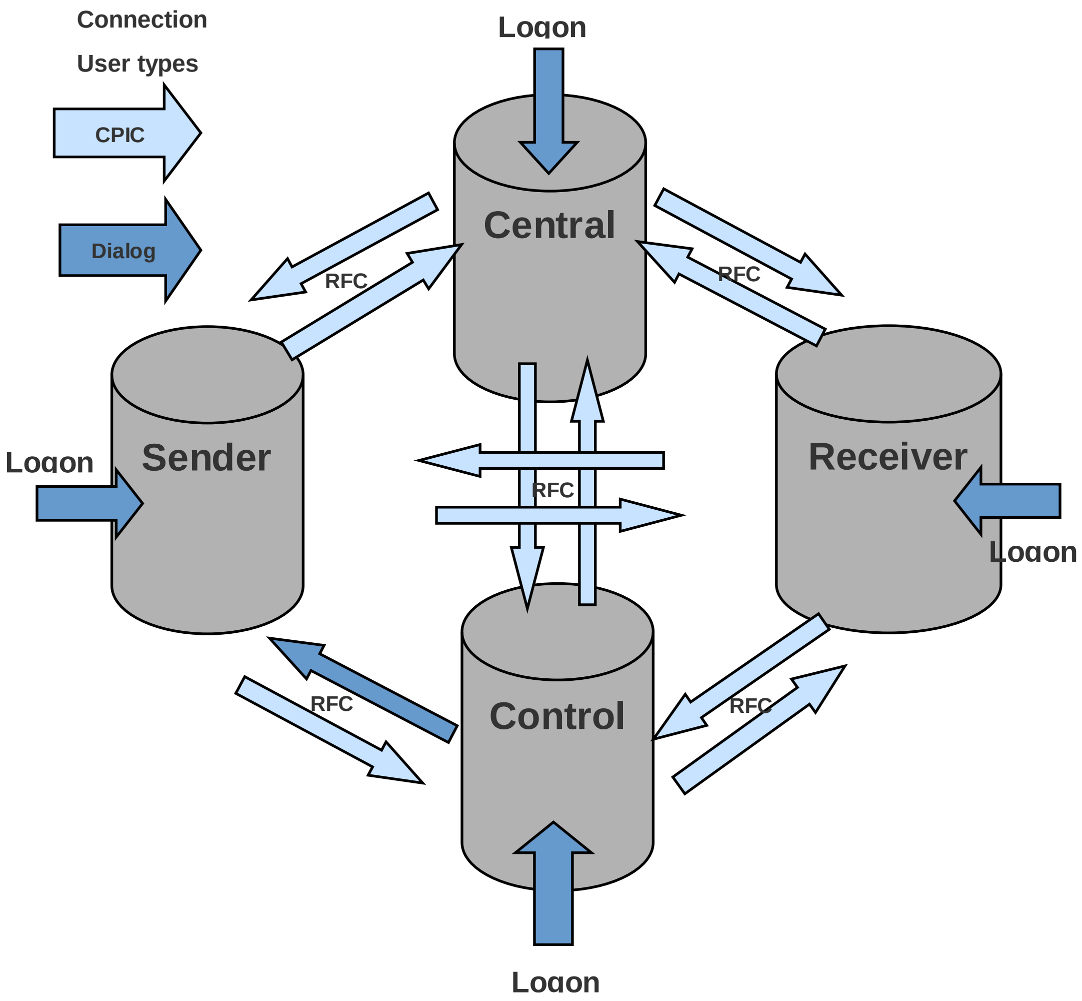
The figure below shows an overview of the **typical technical system landscape for SAP TDMS**.



Logon to each of the systems is required at least for the system administrator so that the corresponding users can be created. Logon to the control system is required for the migration activities. Passwords for users have to be stored in the destination definition.

After creation of communication users and RFC destinations in the control system, destinations are automatically created in the other systems.

For the process type for copying **business process library** objects, the system landscape looks slightly different:



Logon to each of the systems is required at least for the system administrator so that the corresponding users can be created. Logon to the control system is required for the migration activities. Passwords for users have to be stored in the destination definition.

The RFC connection from the control system to the sender system needs to be defined with a dialog user.

After creation of communication users and RFC destinations in the control system, destinations are automatically created in the other systems.

Once the system landscape and the RFC connections have been set up, all actions (except a few postprocessing tasks) in the different systems are triggered and controlled exclusively through the control system. The control system provides a central process control and status management in the process control layer (PCL) of TDMS. Information about all actions (status information, log information) is stored in the central system **and** in the control system.

The sender system can also serve as the central system if it is on basis release 620 or higher. Any of the systems except the receiver system may be chosen as control 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.

In TDMS for HCM projects, and if the control system is **not** also 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.

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.

More Information About the Technical System Landscape

Topic	**Guide/Tool**
Technical description for SAP TDMS	Master Guide
Security	See under Quick Link service.sap.com/security

User Administration and Authentication

SAP TDMS 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 (SAP Library) 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.

For accessing the different systems via Remote Function Call (RFC), a specific user type called **communication user** (CPIC) is required. A communication user can access a system exclusively via 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 Web AS ABAP Security Guide.

The following security measures apply with regard to user management for SAP TDMS:

- Logon to each system is required to create the corresponding CPIC users at least for the administrator of the respective system.
- Logon to control system is required to perform the migration steps.
- RFC destinations are assigned to **one** migration subproject, that is, to one sender – receiver combination.
- Passwords for users have to be stored in the destination definition.
- After creation of communication users and RFC destinations in the control system, the destinations are automatically created in the other systems.

User-related information from the sender system is **not** transferred to the receiver system, so that the users and authorizations in the receiver system can be defined separately as required and will not be 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 to avoid confusion.

Irrespective of all security measures, the users who have access to the control system will necessarily have (indirect) access to the production data in the sender system and may be able to see information stored there. Consequently, we recommend that you keep the number of users in the control system as small as possible to preclude unauthorized access to production data.

Authorizations

TDMS comes with its own authorization object, which is called S_DMIS.

> The authorization concept for SAP TDMS builds on the 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_HCM_MASTER.

Authorization Levels

Authorizations within SAP TDMS can be defined at the following levels:

- Migration **Project**: Within SAP TDMS, a project is a compilation of one or more subprojects which are related from a technical or content point of view.
- Migration **Subproject**: Within SAP TDMS, a subproject defines a combination of a sender system, a receiver system, and the RFC connection between them. If it makes sense from an organizational perspective, more than one subproject can be created for a given combination.
- Migration **Package**: Within SAP TDMS, a package is an instance of a given transfer constellation. That is, a new package needs to be created for every execution of TDMS, no matter if it is for configuring a new constellation or for a refresh.

Authorizations at 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 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, hence any user can execute any activity in the process tree.

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

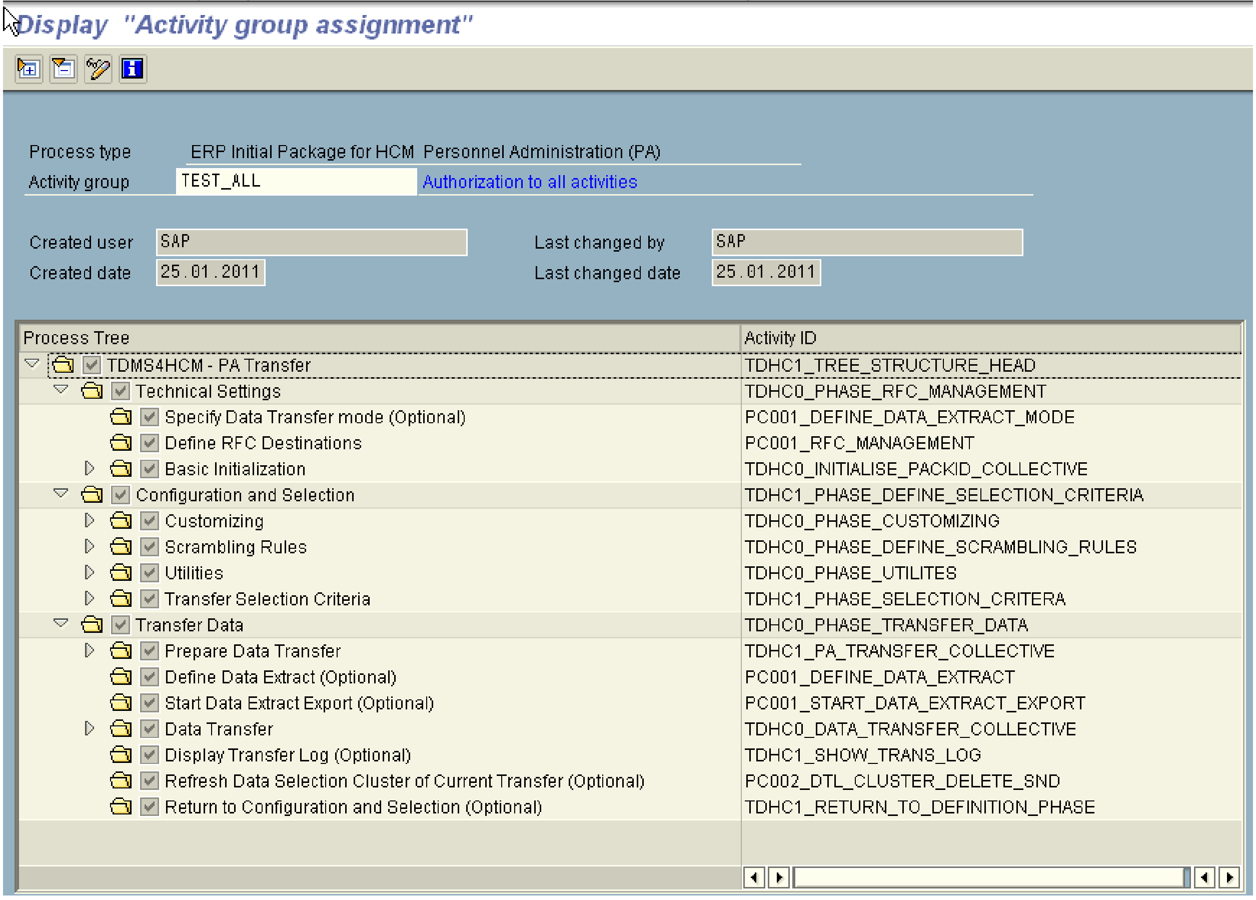
Note

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

Create activity groups TEST_ALL, TEST_CUST, TEST_DEF. Create users TEST-ALL, TEST-CUST, TEST-DEF. create and assign roles ZTDMS_TEST_ALL, ZTDMS_TEST_CUST, ZTDMS_TEST_DEF.

Go to transaction **CNVMBTACTGRP** and enter the Activity Group TEST_ALL. This activity group will have the authorization to execute the complete process tree. Assign **all** the activities to this group. Now, the authorization model become operational.



Display "Activity group assignment"

Process type: ERP Initial Package for HCM Personnel Administration (PA)

Activity group: TEST_ALL Authorization to all activities

Created user: SAP

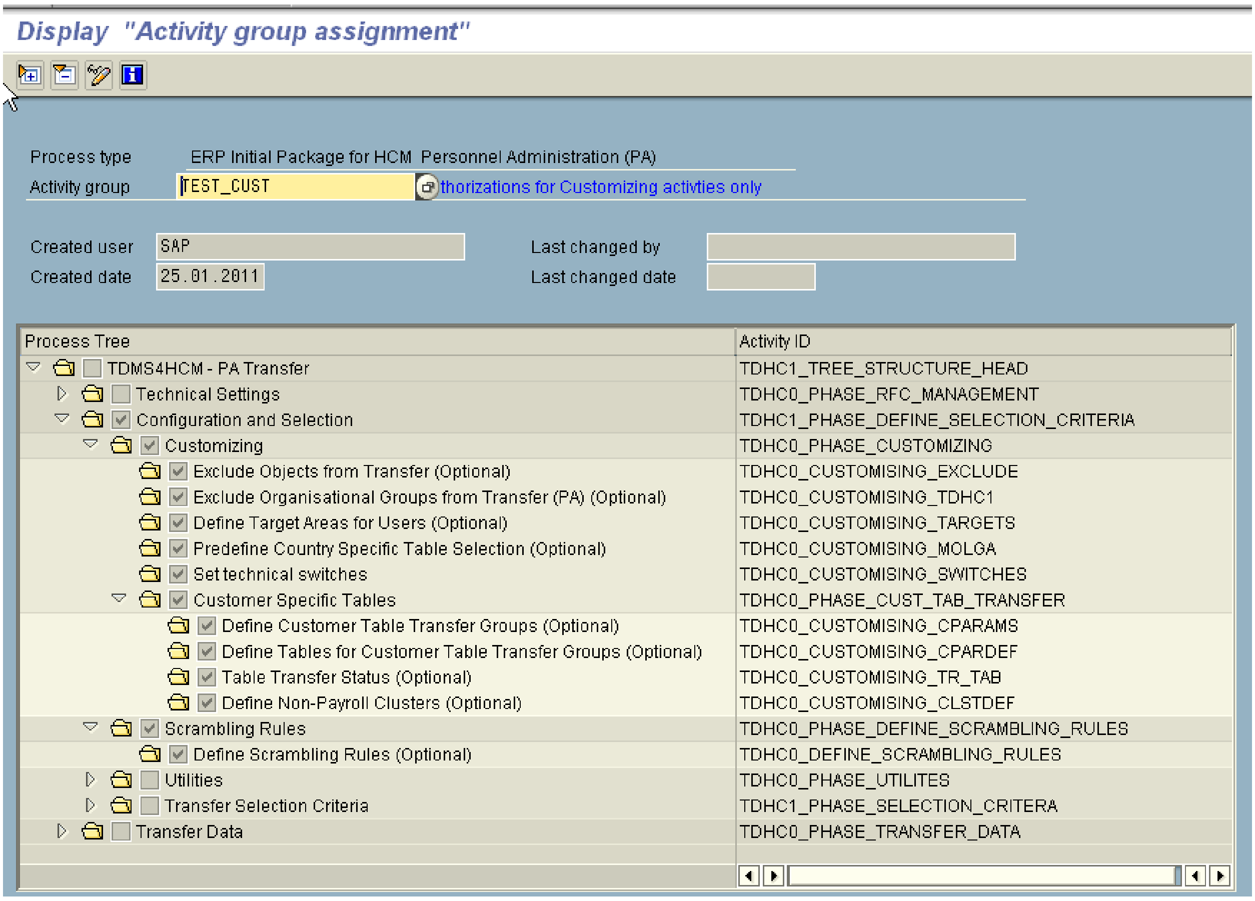
Created date: 25.01.2011

Last changed by: SAP

Last changed date: 25.01.2011

Process Tree	Activity ID
▽ ☑ TDMS4HCM - PA Transfer	TDHC1_TREE_STRUCTURE_HEAD
▽ ☑ Technical Settings	TDHC0_PHASE_RFC_MANAGEMENT
☑ Specify Data Transfer mode (Optional)	PC001_DEFINE_DATA_EXTRACT_MODE
☑ Define RFC Destinations	PC001_RFC_MANAGEMENT
▷ ☑ Basic Initialization	TDHC0_INITIALISE_PACKID_COLLECTIVE
▽ ☑ Configuration and Selection	TDHC1_PHASE_DEFINE_SELECTION_CRITERIA
▷ ☑ Customizing	TDHC0_PHASE_CUSTOMIZING
▷ ☑ Scrambling Rules	TDHC0_PHASE_DEFINE_SCRAMBLING_RULES
▷ ☑ Utilities	TDHC0_PHASE_UTILITES
▷ ☑ Transfer Selection Criteria	TDHC1_PHASE_SELECTION_CRITERA
▽ ☑ Transfer Data	TDHC0_PHASE_TRANSFER_DATA
▷ ☑ Prepare Data Transfer	TDHC1_PA_TRANSFER_COLLECTIVE
☑ Define Data Extract (Optional)	PC001_DEFINE_DATA_EXTRACT
☑ Start Data Extract Export (Optional)	PC001_START_DATA_EXTRACT_EXPORT
▷ ☑ Data Transfer	TDHC0_DATA_TRANSFER_COLLECTIVE
☑ Display Transfer Log (Optional)	TDHC1_SHOW_TRANS_LOG
☑ Refresh Data Selection Cluster of Current Transfer (Optional)	PC002_DTL_CLUSTER_DELETE_SND
☑ Return to Configuration and Selection (Optional)	TDHC1_RETURN_TO_DEFINITION_PHASE

Enter the Activity Group TEST_CUST. This activity group will have the authorization to execute the **customizing activities** only. Assign the respective activities to this group.



Display "Activity group assignment"

Process type ERP Initial Package for HCM Personnel Administration (PA)

Activity group TEST_CUST thorizations for Customizing activties only

Created user SAP

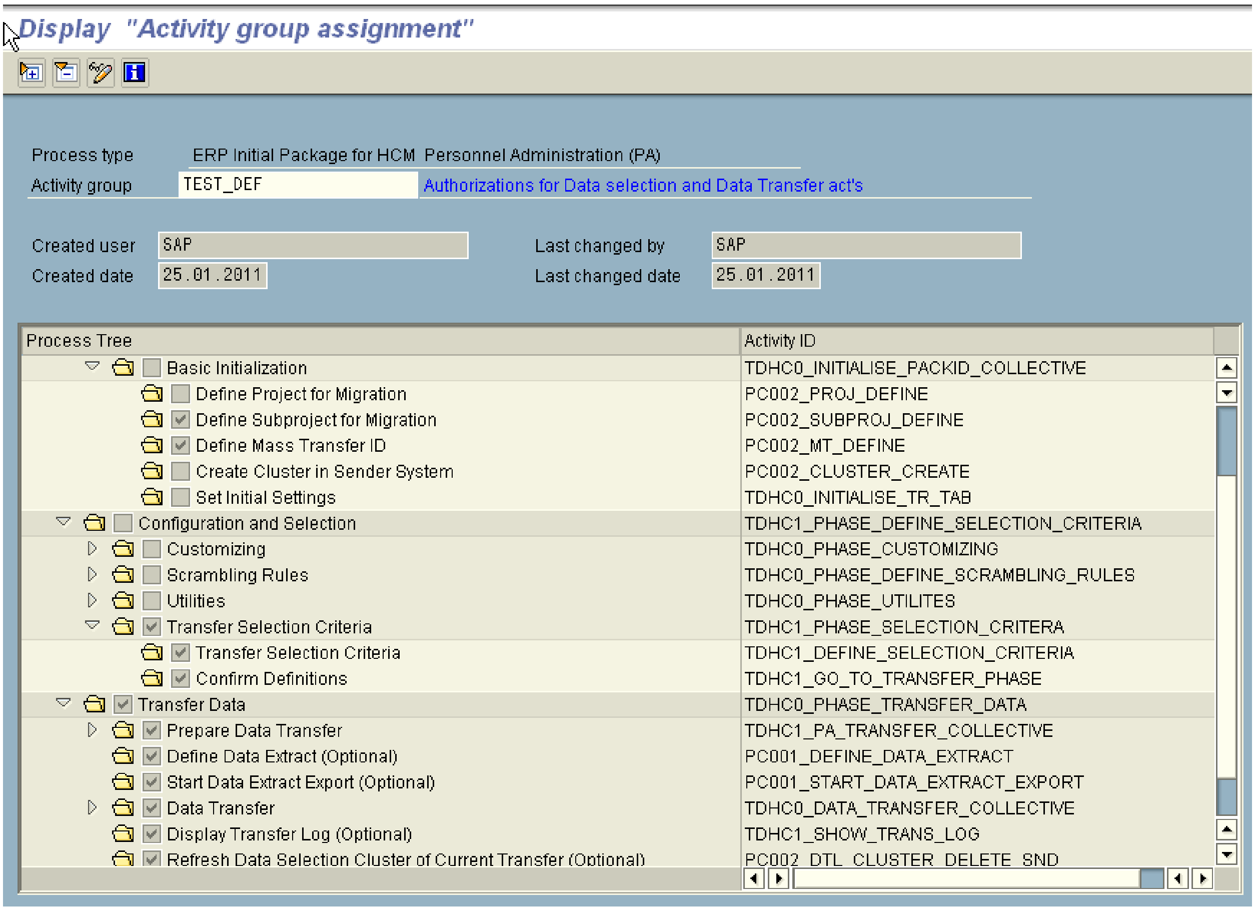
Created date 25.01.2011

Last changed by

Last changed date

Process Tree	Activity ID
☐ TDMS4HCM - PA Transfer	TDHC1_TREE_STRUCTURE_HEAD
☐ Technical Settings	TDHC0_PHASE_RFC_MANAGEMENT
☑ Configuration and Selection	TDHC1_PHASE_DEFINE_SELECTION_CRITERIA
☑ Customizing	TDHC0_PHASE_CUSTOMIZING
☑ Exclude Objects from Transfer (Optional)	TDHC0_CUSTOMISING_EXCLUDE
☑ Exclude Organisational Groups from Transfer (PA) (Optional)	TDHC0_CUSTOMISING_TDHC1
☑ Define Target Areas for Users (Optional)	TDHC0_CUSTOMISING_TARGETS
☑ Predefine Country Specific Table Selection (Optional)	TDHC0_CUSTOMISING_MOLGA
☑ Set technical switches	TDHC0_CUSTOMISING_SWITCHES
☑ Customer Specific Tables	TDHC0_PHASE_CUST_TAB_TRANSFER
☑ Define Customer Table Transfer Groups (Optional)	TDHC0_CUSTOMISING_CPARAMS
☑ Define Tables for Customer Table Transfer Groups (Optional)	TDHC0_CUSTOMISING_CPARDEF
☑ Table Transfer Status (Optional)	TDHC0_CUSTOMISING_TR_TAB
☑ Define Non-Payroll Clusters (Optional)	TDHC0_CUSTOMISING_CLSTDEF
☑ Scrambling Rules	TDHC0_PHASE_DEFINE_SCRAMBLING_RULES
☑ Define Scrambling Rules (Optional)	TDHC0_DEFINE_SCRAMBLING_RULES
☐ Utilities	TDHC0_PHASE_UTILITES
☐ Transfer Selection Criteria	TDHC1_PHASE_SELECTION_CRITERA
☐ Transfer Data	TDHC0_PHASE_TRANSFER_DATA

Enter the Activity Group TEST_DEF. This activity group will have the authorization to execute the **data selection and data transfer** activities. Assign the respective activities to this group.



Display "Activity group assignment"

Process type ERP Initial Package for HCM Personnel Administration (PA)

Activity group TEST_DEF Authorizations for Data selection and Data Transfer act's

Created user SAP

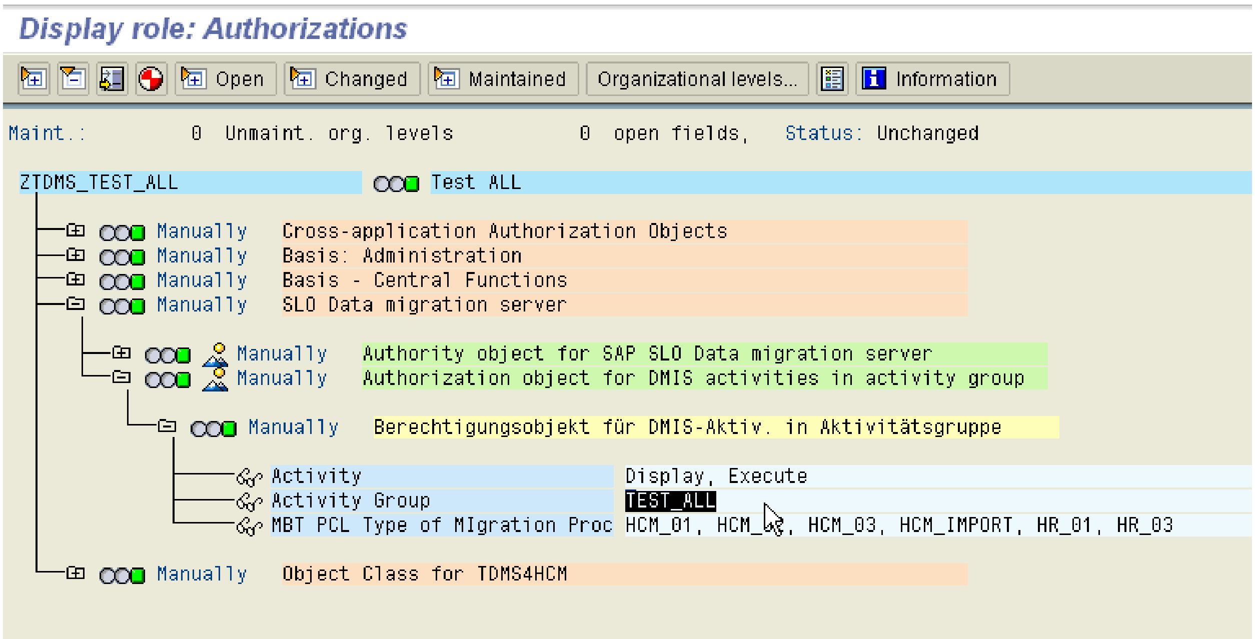
Created date 25.01.2011

Last changed by SAP

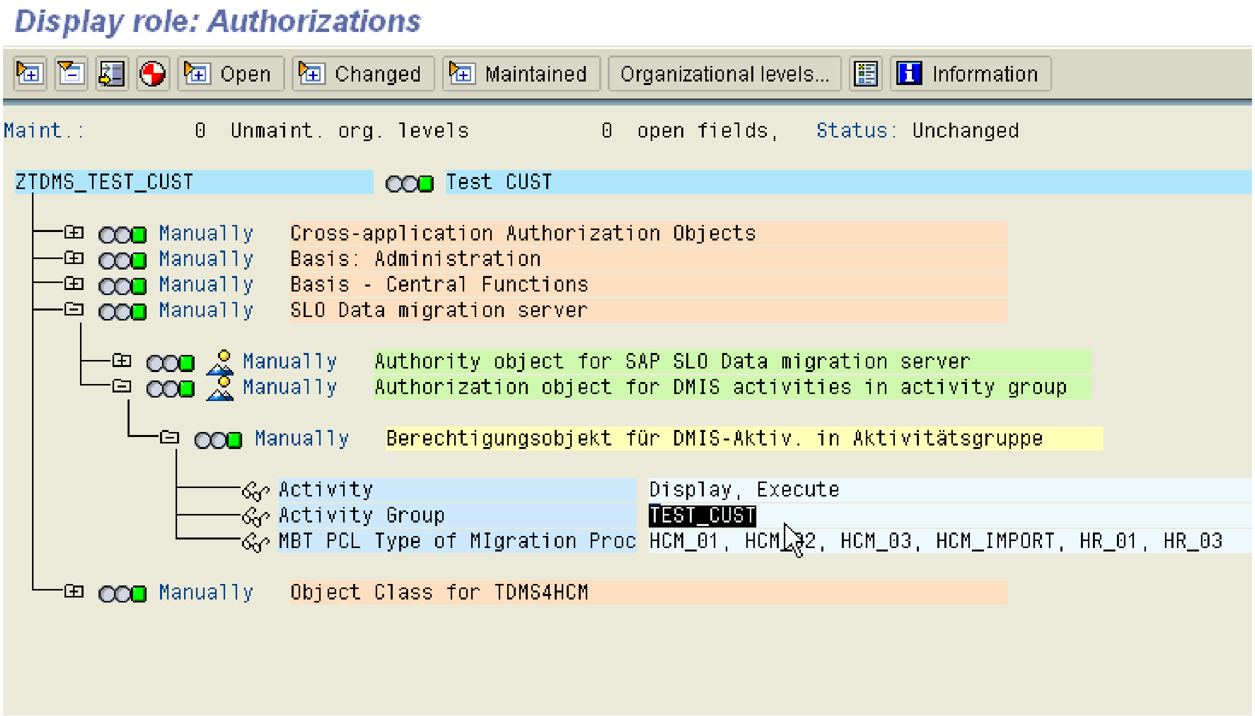
Last changed date 25.01.2011

Process Tree	Activity ID
▽ □ Basic Initialization	TDHC0_INITIALISE_PACKID_COLLECTIVE
□ Define Project for Migration	PC002_PROJ_DEFINE
☑ Define Subproject for Migration	PC002_SUBPROJ_DEFINE
☑ Define Mass Transfer ID	PC002_MT_DEFINE
□ Create Cluster in Sender System	PC002_CLUSTER_CREATE
□ Set Initial Settings	TDHC0_INITIALISE_TR_TAB
▽ □ Configuration and Selection	TDHC1_PHASE_DEFINE_SELECTION_CRITERIA
▷ □ Customizing	TDHC0_PHASE_CUSTOMIZING
▷ □ Scrambling Rules	TDHC0_PHASE_DEFINE_SCRAMBLING_RULES
▷ □ Utilities	TDHC0_PHASE_UTILITES
▽ ☑ Transfer Selection Criteria	TDHC1_PHASE_SELECTION_CRITERA
☑ Transfer Selection Criteria	TDHC1_DEFINE_SELECTION_CRITERIA
☑ Confirm Definitions	TDHC1_GO_TO_TRANSFER_PHASE
▽ ☑ Transfer Data	TDHC0_PHASE_TRANSFER_DATA
▷ ☑ Prepare Data Transfer	TDHC1_PA_TRANSFER_COLLECTIVE
☑ Define Data Extract (Optional)	PC001_DEFINE_DATA_EXTRACT
☑ Start Data Extract Export (Optional)	PC001_START_DATA_EXTRACT_EXPORT
▷ ☑ Data Transfer	TDHC0_DATA_TRANSFER_COLLECTIVE
☑ Display Transfer Log (Optional)	TDHC1_SHOW_TRANS_LOG
☑ Refresh Data Selection Cluster of Current Transfer (Optional)	PC002_DTL_CLUSTER_DELETE_SND

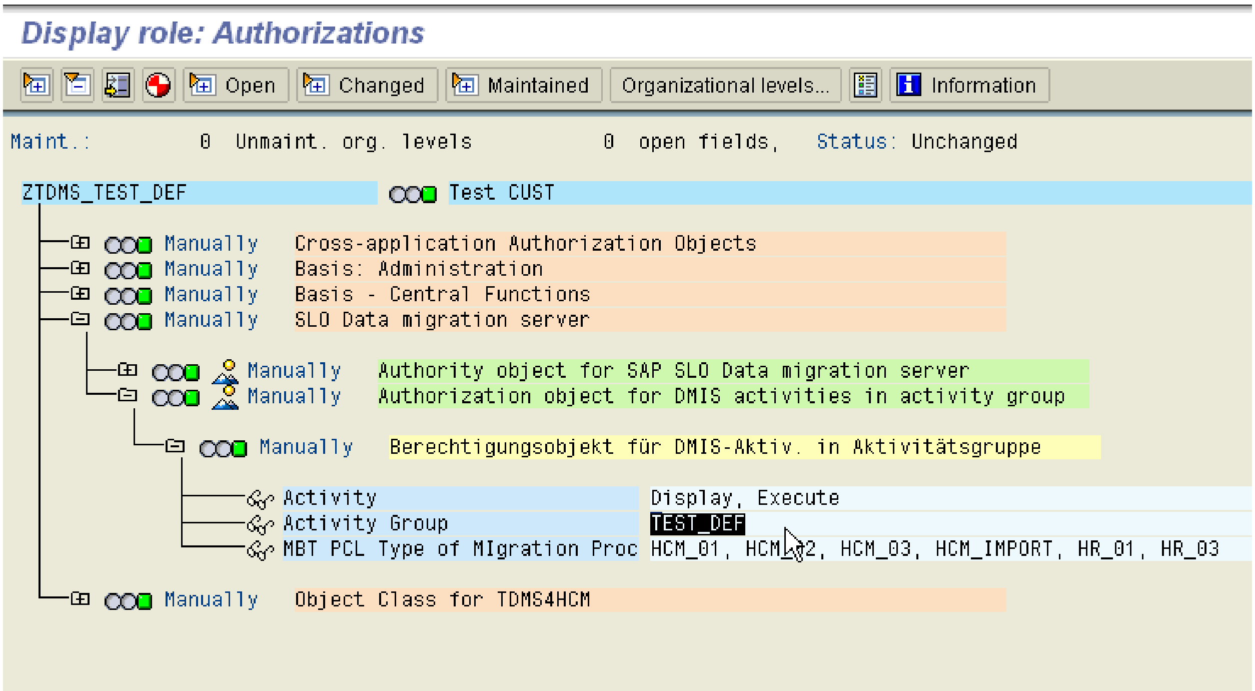
Assign the activity groups to respective roles



```
Maint.:          0 Unmaint. org. levels          0 open fields,   Status: Unchanged

ZTDMS_TEST_ALL             Test ALL
   Manually   Cross-application Authorization Objects
   Manually   Basis: Administration
   Manually   Basis - Central Functions
   Manually   SLO Data migration server
      Manually   Authority object for SAP SLO Data migration server
      Manually   Authorization object for DMIS activities in activity group
         Manually   Berechtigungsobjekt für DMIS-Aktiv. in Aktivitätsgruppe
            Activity                       Display, Execute
            Activity Group                 TEST_ALL
            MBT PCL Type of MIgration Proc HCM_01, HCM_02, HCM_03, HCM_IMPORT, HR_01, HR_03
   Manually   Object Class for TDMS4HCM
```

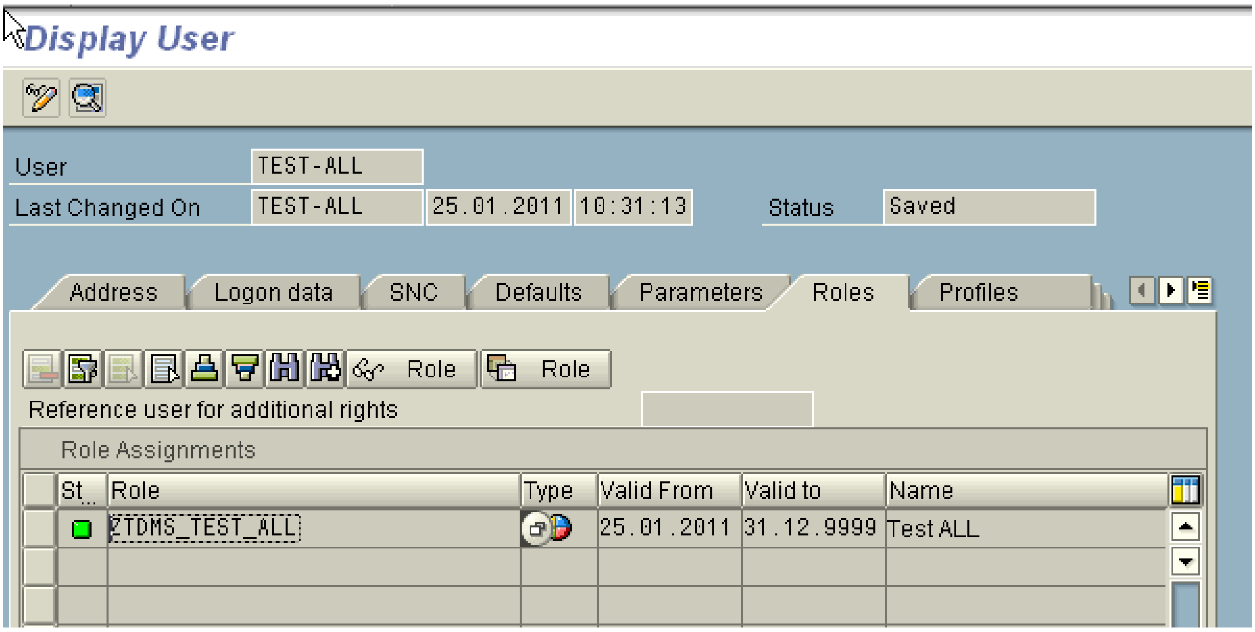


```
Maint.:          0 Unmaint. org. levels          0 open fields,   Status: Unchanged

ZTDMS_TEST_CUST            Test CUST
   Manually   Cross-application Authorization Objects
   Manually   Basis: Administration
   Manually   Basis - Central Functions
   Manually   SLO Data migration server
      Manually   Authority object for SAP SLO Data migration server
      Manually   Authorization object for DMIS activities in activity group
         Manually   Berechtigungsobjekt für DMIS-Aktiv. in Aktivitätsgruppe
            Activity                       Display, Execute
            Activity Group                 TEST_CUST
            MBT PCL Type of MIgration Proc HCM_01, HCM_02, HCM_03, HCM_IMPORT, HR_01, HR_03
   Manually   Object Class for TDMS4HCM
```



Display role: Authorizations

```
Maint.:          0  Unmaint. org. levels          0  open fields,   Status: Unchanged

ZTDMS_TEST_DEF                                 Test CUST
  Manually  Cross-application Authorization Objects
  Manually  Basis: Administration
  Manually  Basis - Central Functions
  Manually  SLO Data migration server
      Manually  Authority object for SAP SLO Data migration server
      Manually  Authorization object for DMIS activities in activity group
          Manually  Berechtigungsobjekt für DMIS-Aktiv. in Aktivitätsgruppe
              Activity                      Display, Execute
              Activity Group                TEST_DEF
              MBT PCL Type of MIgration Proc HCM_01, HCM_02, HCM_03, HCM_IMPORT, HR_01, HR_03
  Manually  Object Class for TDMS4HCM
```



Display User

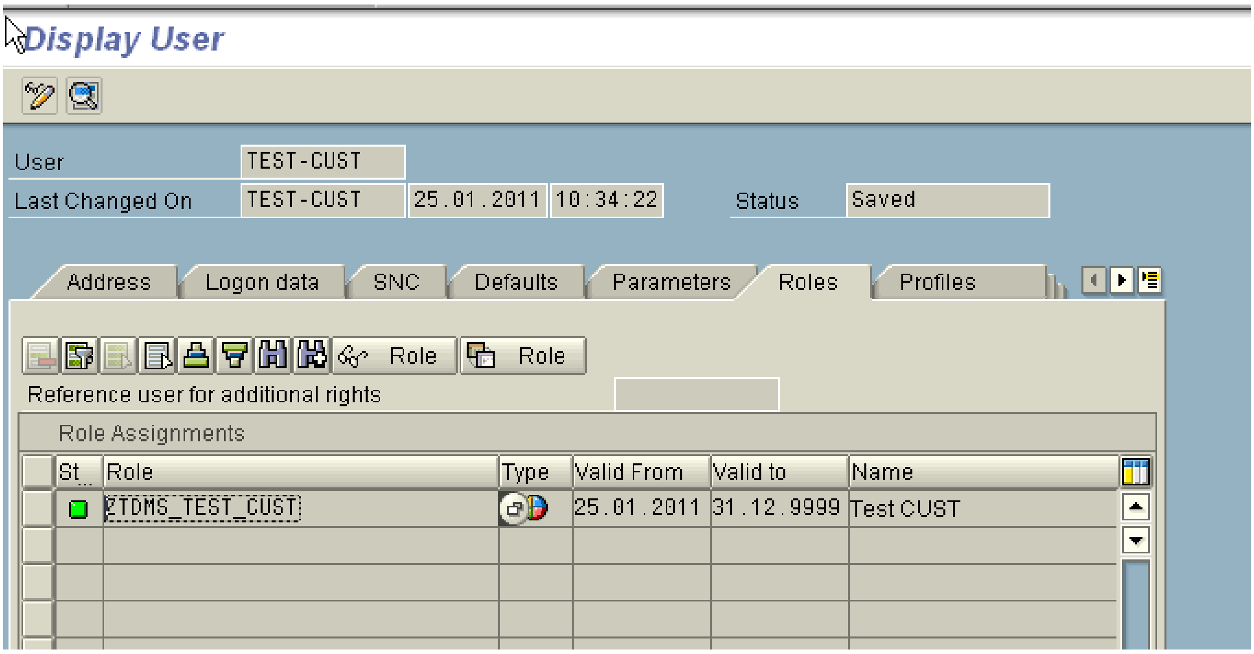
User	TEST-ALL			
Last Changed On	TEST-ALL	25.01.2011	10:31:13	Status: Saved

Reference user for additional rights

Role Assignments

St...	Role	Type	Valid From	Valid to	Name
🟩	ZTDMS_TEST_ALL		25.01.2011	31.12.9999	Test ALL

Assign the roles to respective users



Display User

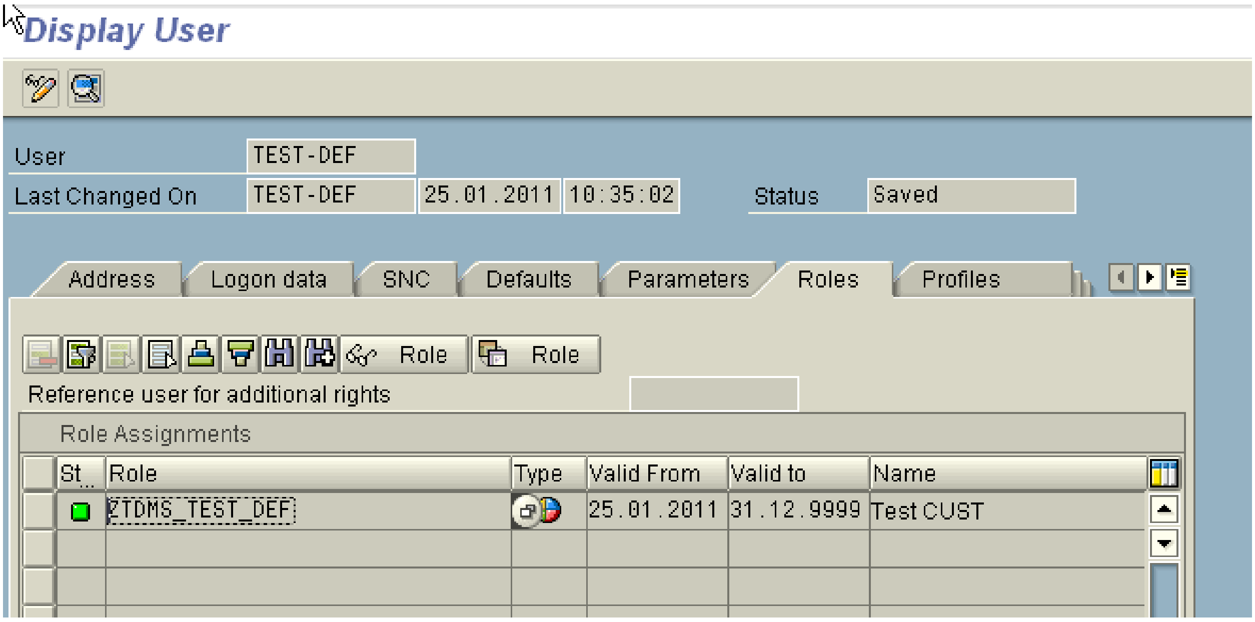
User TEST-CUST

Last Changed On TEST-CUST 25.01.2011 10:34:22 Status Saved

Reference user for additional rights

Role Assignments

St..	Role	Type	Valid From	Valid to	Name
🟩	ZTDMS_TEST_CUST		25.01.2011	31.12.9999	Test CUST



Display User

User TEST-DEF

Last Changed On TEST-DEF 25.01.2011 10:35:02 Status Saved

Reference user for additional rights

Role Assignments

St..	Role	Type	Valid From	Valid to	Name
🟩	ZTDMS_TEST_DEF		25.01.2011	31.12.9999	Test CUST

User Roles

From an **organizational** perspective, there are the following user roles:

- Migration Master (Super user)
- Migration Lead
- Migration User
- Migration Guest

The main differences between the user roles are as follows:

	Lead	User	Guest
Project	Create projects/ delete one's own projects	Work in packages in assigned projects	Display activities in all packages in assigned projects
Subproject	Create subprojects/ delete one's own subprojects in assigned projects	Work in packages in assigned subprojects	Display activities in all packages in assigned subproject
Package	Create packages/ delete one's own packages in assigned subprojects	Work in assigned packages	Display activities of assigned packages

From a **technical** perspective, there are the following user roles, which are automatically made available in all systems where the respective TDMS add-on is installed:

- The add-on DMIS includes the following roles:
    - SAP_DMIS_MASTER
    - SAP_TDMS_MASTER
    - SAP_TDMS_PROJECT_LEAD_USER
    - SAP_TDMS_SUBPROJECT_LEAD_USER
    - SAP_TDMS_PACKAGE_LEAD_USER
    - SAP_TDMS_USER
    - SAP_TDMS_DISPLAY_USER
    - SAP_TDMS_ACTGROUP_ADMIN
    - SAP_TDMS_ACTGROUP_DISPLAY_USER
    - SAP_TDMS_ACTGROUP_EXEC
- The add-on DMIS_EXT includes the following roles:
    - SAP_DMIS_EXT_DD_ALL
    - SAP_DMIS_EXT_DD_M_ALL
    - SAP_DMIS_EXT_DD_RFC
- The add-on DMIS_HR comes with one additional role called SAP_TDMS_HCM_MASTER, which includes the specific authorizations a user needs in the sender system in the context of SAP TDMS for HCM. For more detailed information, see the description that is shipped with the role.

For an overview of the actions that users can perform with the different roles contained in add-on DMIS, see the appendix.

In addition, the following **composite roles** come with add-on DMIS_EXT:

- SAP_TDMS_MASTER_EXT:
  Contains the authorizations that are assigned to the following roles:
    - SAP_TDMS_MASTER
    - SAP_DMIS_EXT_DD_ALL

    - SAP_DMIS_EXT_DD_M_ALL
    - SAP_DMIS_EXT_DD_RFC

- SAP_TDMS_PROJECT_LEAD_USER_EXT
  Contains the authorizations that are assigned to the following roles:
    - SAP_TDMS_PROJECT_LEAD_USER
    - SAP_DMIS_EXT_DD_ALL
    - SAP_DMIS_EXT_DD_M_ALL
    - SAP_DMIS_EXT_DD_RFC

- SAP_TDMS_SUBPROJ_LEAD_USER_EXT
  Contains the authorizations that are assigned to the following roles:
    - SAP_TDMS_SUBPROJECT_LEAD_USER
    - SAP_DMIS_EXT_DD_ALL
    - SAP_DMIS_EXT_DD_M_ALL
    - SAP_DMIS_EXT_DD_RFC

- SAP_TDMS_PACKAGE_LEAD_USER_EXT
  Contains the authorizations that are assigned to the following roles:
    - SAP_TDMS_PACKAGE_LEAD_USER
    - SAP_DMIS_EXT_DD_ALL
    - SAP_DMIS_EXT_DD_M_ALL
    - SAP_DMIS_EXT_DD_RFC

- SAP_TDMS_USER_EXT
  Contains the authorizations that are assigned to the following roles:
    - SAP_TDMS_USER
    - SAP_DMIS_EXT_DD_ALL
    - SAP_DMIS_EXT_DD_M_ALL
    - SAP_DMIS_EXT_DD_RFC

A user who wants to work with process types contained in DMIS_EXT needs one of these composite roles. The RFC users must have at least the authorizations that are included in role SAP_TDMS_USER_EXT.

SAP TDMS needs the authorization S_DEVELOP, to generate repository objects (like programs, data structures) in all affected systems. These objects are required to read the data in the sender system, scramble the data and export data. Authorization S_DEVELOP is used by a ‘Batch User’ only.

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

User Registration

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

When you register a user, the organizational user role (lead, team or guest) of that user in the given project, subproject or package is determined by the user’s technical user role:

- A user with the role SAP_TDMS_MASTER is automatically registered as migration lead.

- A user with one of the *LEAD* roles is automatically registered as migration lead for the respective level (project, subproject or package).
- A user with the role SAP_TDMS_USER is automatically registered as migration user.
- A user with the role SAP_TDMS_DISPLAY_USER is automatically registered as migration guest.

Registering additional users is the responsibility of the user who created the respective project, subproject or package. The registration at package level also has to be done for users in remote systems. (The registration function includes an option for switching between the systems.)

SAP TDMS also offers functions for locking all non-registered users before the start of the actual data transfer in a migration and unlocking them again afterwards. This is an additional precaution against actions in the system that might interfere with the data transfer.

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

Network and Communication Security

Access to all sender and receiver systems in an SAP TDMS system landscape takes place exclusively through RFC connections. For more information about security issues in connection with RFC, see the relevant sections in SAP Library.

Communication Destinations

Use

TDMS does **not** come with fixed destinations or user names. The following destinations need to be created:

- The control system and the central system must be connected by RFC to all participating systems. Each system must also have a destination directed to itself.
- The sender system and the receiver system must be connected to the control system and the central system. Each system must also have 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 and cannot be changed by standard RFC management means.

> As of SAP NetWeaver 2004s, extended password rules apply. This affects SAP TDMS in the following ways:
>
> - Because passwords are no longer supposed to be transferred directly, the automatic distribution and synchronization process described above does not work for SAP NetWeaver 2004s.
>   To establish the RFC connections, you need to enter the passwords manually in each of the systems. Alternatively, you can decide to allow unencrypted transmission of the passwords for the RFC connections, but you need to be aware that this goes against SAP's explicit security recommendations.
>   For more information, see the RFC/ICF Security Guide.
> - The maximum length of the passwords has been extended, and the passwords are case-sensitive. However SAP TDMS still accepts only passwords with eight or fewer characters in upper case.

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

- Any change of a RFC destination that is 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 – or SAP_TDMS_USER_EXT, respectively, for DMIS_EXT.
- 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.

Data Storage Security

In connection with TDMS, no sensitive data is created or stored temporarily.

Trace and Log Files

No trace files are written for TDMS.

Log files (application log) are written for each activity within TDMS. These logs show which user ececuted a given activity at what time and for which system(s). The log files can be accessed via the procedure monitor for TDMS.

Appendix

Actions a user can carry out depending on the user role:

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

Action	SAP_TDMS_MASTER	SAP_TDMS_PROJECT_LEAD_USER	SAP_TDMS_SUBPROJECT_LEAD_USER	SAP_TDMS_PACKAGE_LEAD_USER	SAP_TDMS_USER	SAP_TDMS_DISPLAY_USER
Create Project	X	X				
Delete Project	X	X				
Create Subproject	X	X	X			
Delete Subproject	X	X	X			
Create Package	X	X	X	X		
Deactivate Package	X	X	X			
Copy Package	X	X	X			
View Migration overview TDMS						
View Package process tree	X	X	X	X	X	X
View procedure monitor	X	X	X	X	X	X
Register project users	X	X				
Register subproject users	X	X	X			
Register package users	X	X	X	X		
Lock users	X	X	X	X		
Unlock users	X	X	X	X		
Maintain RFC destinations	X	X	X	X		
Synchronize RFC destinations	X	X	X	X		

Action	SAP_TDMS_MASTER	SAP_TDMS_PROJECT_LEAD_USER	SAP_TDMS_SUBPROJECT_LEAD_USER	SAP_TDMS_PACKAGE_LEAD_USER	SAP_TDMS_USER	SAP_TDMS_DISPLAY_USER
Lock RFC destination	X	X	X	X		
Unlock RFC destination	X	X	X	X		
Start Activity	X	X	X	X	X	
Maintain technical settings	X	X	X	X	X	
Call DTL function	X	X	X	X	X	