

Security Guide for SAP Landscape Transformation 2.0



Version 2.9.1 December 2015



Copyright

© Copyright 2015 SAP AG. All rights reserved.

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

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

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

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

Oracle is a registered trademark of Oracle Corporation.

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

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

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

Java is a registered trademark of Sun Microsystems, Inc.






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

MaxDB is a trademark of MySQL AB, Sweden.

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

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

Icons in Body Text

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
<i>Example text</i>	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	5
Before You Start.....	7
Technical System Landscape	8
User Administration and Authentication.....	11
Authorizations	12
Network and Communication Security.....	21
Communication Destinations	21
Data Storage Security	27
Trace and Log Files	28



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 SAP Landscape Transformation. SAP Landscape Transformation can involve changes to production data, and transferring data from the production system (or a system that is a recent copy of the production system) to other production systems. Consequently, security issues that need to be considered for SAP Landscape Transformation include data protection (sensitive data), secure connections between systems, and authorizations. To assist you in securing SAP Landscape Transformation, we provide this security guide.

About this Document

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

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 Landscape Transformation.

- **User Administration and Authentication**

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

- User types that are required by SAP Landscape Transformation
- User roles that are delivered with SAP Landscape Transformation
- User registration within SAP Landscape Transformation

- **Authorizations**

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

- **Session Security Protection**

This section provides the recommendation to use SSL.

- **Network and Communication Security**

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

- **Internet Communication Framework Security**

This section provides an overview of the SICF services that need to be activated.

- **Data Storage Security**

This section provides an overview of any critical data that is used by SAP Landscape Transformation 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 occurs.

- **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 service.sap.com/securityguide on the SAP Service Marketplace. The current version of the SAP NetWeaver security guide, which deals with general security issues, is also available in this location.

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
Security	http://sdn.sap.com/irj/sdn/security
Security Guides	http://service.sap.com/securityguide
Related SAP Notes	http://support.sap.com/notes http://support.sap.com/securitynotes
Released platforms	http:// support.sap.com/pam
Network security	http://service.sap.com/securityguide
SAP Solution Manager	http://support.sap.com/solutionmanager

Add-On Structure for SAP Landscape Transformation

For SAP Landscape Transformation, you need the following add-ons:

- DMIS_2011 (for more information, see SAP Note 1577441)
- SHC_CONT_2011(for more information, see SAP Note 1618947)

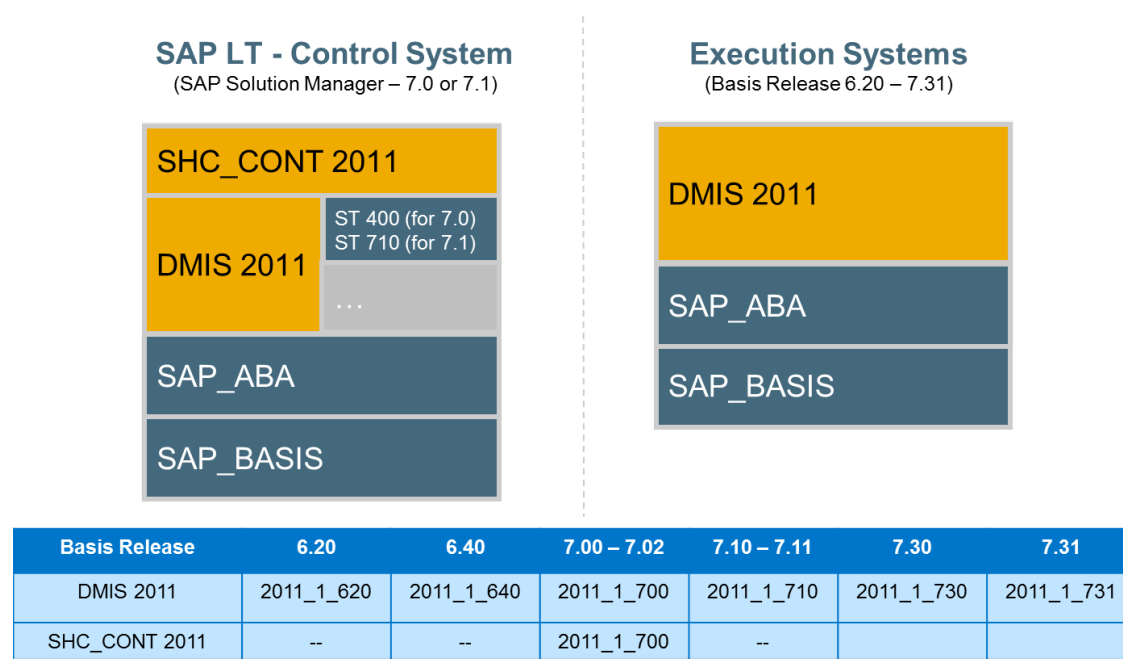
This information is important in a security context because user roles and related settings and functions are included in these add-ons.

Technical System Landscape

SAP Landscape Transformation runs on a SAP Solution Manager system. The SAP Solution Manager system represents the control system that you use to manage an SAP Landscape Transformation project. Both add-ons (DMIS 2011; SHC_CONT_2011) must be installed in order to use the functionality provided with the SAP Landscape Transformation work center. For the add-on SHC_CONT_2011, SAP Solution Manager (ST_400) with SP15 is a technical prerequisite – however no additional basis configuration within SAP Solution Manager is required to get started with SAP Landscape Transformation software.

In the other SAP systems affected by the SAP landscape transformation project (execution systems), only the installation of add-on DMIS 2011 is required. The affected systems must be between release 6.20 and 710.

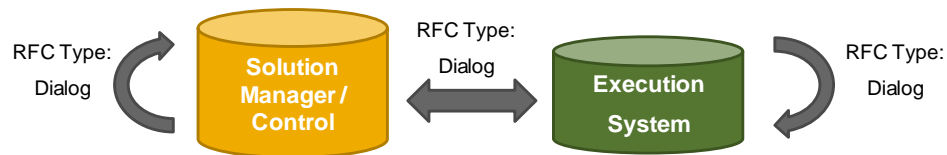
In general, no specific basic configuration is required for SAP Landscape Transformation software beside the assignment of SAP LT role(s) and respective authorizations for users.



Different technical system landscapes are required for the transformation solutions that are part of SAP Landscape Transformation 2.0.

System Landscape with Control (Solution Manager) and Execution System

For transformation solutions which require only two systems (for example chart of accounts conversion, company code deletion and most analyses), the following system landscape is required.

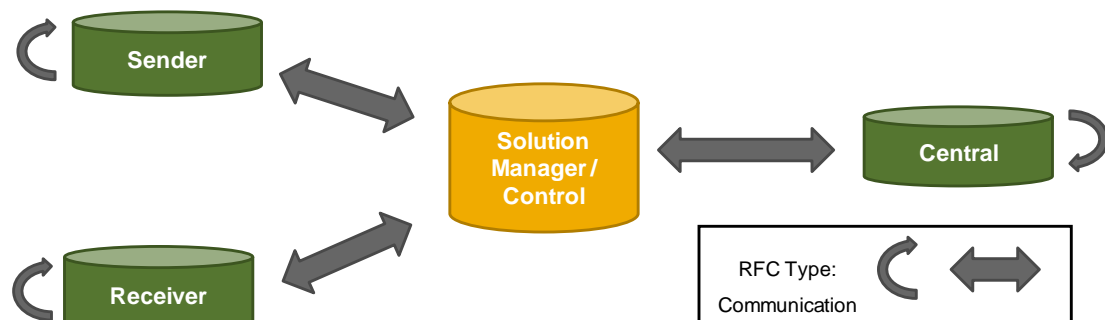


For every connection from the Solution Manger/control system to the execution system and backwards, a RFC connection with a dialog user is required. In addition, an RFC connection which points to the system itself is required.

System Landscape for Client Transfer without Upgrade

For a client transfer without an upgrade, RFC connections to a sender, receiver and central system are required.

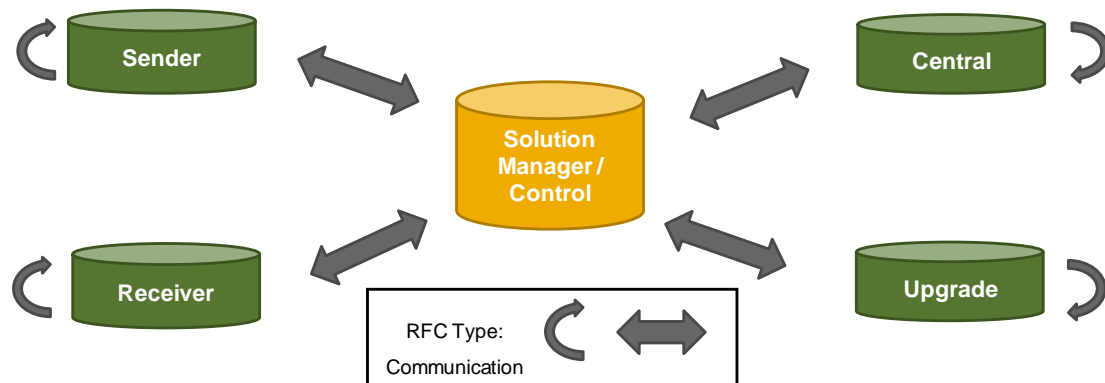
In addition, the control system must also have a destination that is directed to itself (note that the use of the destination *NONE* is not possible). All RFC connections must be of type *Communication*.



System Landscape for Client Transfer with Upgrade

For a client transfer that involves an upgrade, RFC connections to a sender, receiver, upgrade, and central system are necessary.

In addition, the control system must also have a destination that is directed to itself (note that the use of the destination *NONE* is not possible). All RFC connections must be of type *Communication*.



Note: The system landscape configuration within SAP Landscape Transformation 2.0 supports the creation and distribution of required RFC connections.

Once the RFC connections have been set up, they can be used in a SAP Landscape Transformation project.



User Administration and Authentication

SAP Landscape Transformation 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 Landscape Transformation.

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

For accessing the different systems by remote function call (RFC), depending on the transformation scenario, a communication user or a dialog user is required. A communication user can access a system exclusively by RFC and cannot execute steps in dialog mode directly in a system. A dialog user can execute steps 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 Landscape Transformation:

- Logon to each system is required to create the corresponding users at least for the administrator of the respective system.
- Logon to Solution Manager System is required to create a project and perform corresponding steps.

Irrespective of all security measures, the users who have access to the control system will 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 low as possible to preclude unauthorized access to production data.



Authorizations

SAP Landscape Transformation uses a combined user registration and authorization concept. Authorizations that are available in a user profile control the actions that a user is authorized to perform.

Authorization Objects

SAP Landscape Transformation comes with its own authorization objects:

Class: **DMIS**

- **S_DMIS - SLO Data Migration Server**

Description: Authority object for SAP SLO Data migration

Authorization fields

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_PR_LEV	MBT PCL: Processing Role Level
ACTVT	Activity

- **S_DMIS_ACT**

Description: Authorization object for activity group maintenance

Authorization fields

Field name	Heading
PROC_TYPE	MBT PCL Type of Migration Process
ACTVT	Activity

- **S_DMIS_ANA**

Description: DMIS Analysis Authorizations

Authorization fields

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_AN_APP	SHC: Analysis application
ACTVT	Activity

- **S_DMIS_ADV**

Description: DMIS Analysis Development authorization

Authorization fields

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_AN_APP	SHC: Analysis application ID
ACTVT	Activity

- **S_DMIS_PPM**

Description: DMIS Portfolio and Project Management authorization

Authorization fields

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_PP_OTY	BTP Technical Object Type
MBT_PP_OBJ	BTP Technical Object Name
ACTVT	Activity

- **S_DMIS_AGR**

Description: Authorization object for DMIS activities in activity group

Authorization fields

Field name	Heading
ACT_GRP	Activity Group
PROC_TYPE	MBT PCL Type of Migration Process
ACTVT	Activity

- **S_DMIS_DEV**

Description: Development authority for DMIS

Authorization fields

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_PR_NSP	MBT PCL Development Namespace
ACTVT	Activity

- **S_DMIS_PDV**

Description: DMIS Portfolio Object Development

Authorization fields

Field name	Heading
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

ACTVT	Activity
-------	----------

- **S_DMIS_SCR**

Description: Authorization Object for Scrambling

Authorization fields

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_PR_LEV	MBT PCL: Processing Role Level
ACTVT	Activity

Class: **AAAB - Cross-Application Authorization Objects**

- **S_DMC_S_R**

Authorization fields

Field name	Heading
ACTVT	Activity

- **S_DMC_ADMI**

Description: DMC: Administration activities

Authorization fields

Field name	Heading
TCD	Transaction Code
DMC_OBJECT	Activity
DMC_CNLACTION	Activity
DMC_CUSACTION	Activity
DMC_ADMACTION	Activity

- **S_DMC_COBJ**

Description: DMC: Conversion Object activities

Authorization fields

Field name	Heading
TCD	Transaction Code
DMC_OBJECT	Activity
DMC_CNLACTION	Activity
DMC_CUSACTION	Activity
DMC_ADMACTION	Activity

- **S_DMC_ORGO**

Description: DMC: Organizational Object Activities

Authorization fields

Field name	Heading
DMC_PRJCT	Project IDs
DMC_SPRJCT	Subproject IDs
DMC_COBJ	Conversion Object IDs
TCD	Transaction Code

- **S_DMC_PRJC**

Description: DMC: Project activities

Authorization fields

Field name	Heading
TCD	Transaction Code
DMC_OBJECT	Activity
DMC_CNLACT	Activity
DMC_CUSACT	Activity
DMC_ADMACT	Activity

- **S_DMC_SPRJ**

Description: DMC: Subproject activities

Authorization fields

Field name	Heading
TCD	Transaction Code
DMC_OBJECT	Activity
DMC_CNLACT	Activity
DMC_CUSACT	Activity
DMC_ADMACT	Activity

- **S_DMC_SPRJ**

Description: DMC: DMC: Transaction and Activity

Authorization fields

Field name	Heading
TCD	Transaction Code
ACTVT	Activity
DMC_PRJCT	Project IDs
DMC_SPRJCT	Subproject IDs
DMC_COBJ	Conversion Object IDs

User Roles

There are the following user roles for SAP Landscape Transformation:

- **Master** (super user)
Composite role for master users (all authorizations)
- **Guest**
Composite role for users with display only authorizations
- **Business Expert**
Composite role for business expert users without project administration authorizations
- **Technical Execution Expert**
Composite role for technical execution expert users with complete project administration authorizations
- **Technical Execution User**
Composite role for technical execution expert users without project administration authorizations

The main differences between the user roles are as follows:

Area	Action	Guest	Business expert	Technical execution user	Technical execution expert	Master
Overview	Display Overview screen	X	X	X	X	X
Portfolio	Display / Navigate in Portfolio	X	X	X	X	X
Project Templates	Display Project Template Overview	X	X	X	X	X
	Display Project Template	X	X	X	X	X
	Create Project Template	-	X	-	X	X
	Edit Any Other Project Template	-	-	-	-	X
	Edit Own Project Template	-	X	-	X	X
	Delete Any Other Project Template	-	-	-	-	X
	Delete Own Project Template	-	X	-	X	X
Projects	Display List of Projects	X	X	X	X	X
	Display Details of Any Other Project	X	X	X	X	X
	Display Details of Own/Assigned Project	X	X	X	X	X
	Edit Any Other Project	-	-	-	-	X
	Edit Own/Assigned Project	-	X	-	X	X

Area	Action	Guest	Business expert	Technical execution user	Technical execution expert	Master
	Delete Any Other Project	-	-	-	-	X
	Delete Own/Assigned Project	-	X	-	X	X
	Create Project	-	X	-	X	X
	Compose Any Other Project	-	-	-	-	X
	Compose Own/Assigned Project	-	X	-	X	X
	Extend Any Other Project	-	-	-	-	X
	Extend Own/Assigned Project	-	X	-	X	X
	Create / Execute Analysis	-	X	X	X	X
	Evaluate Analysis Results	-	X	X	X	X
	Create Transformation Solution Package	-	-	-	X	X
	Execute Transformation Solution Package	-	X	X	X	X
	Display Transformation Solution Package	X	X	X	X	X

The add-on DMIS_2011 includes the following single roles:

Role Name	Description
SAP_SLOP_MASTER	SAP SLOP - Master user
SAP_SLOP_PROJECT_LEAD	SAP SLOP - Standard project lead user
SAP_SLOP_USER	SAP SLOP - Standard user for execution
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user
SAP_SLOP_DISPLAY_USER	SAP SLOP - Standard user only for display
SAP_LT_WORKCENTER	SAP Landscape Transformation work center
SAP_LT_WORKCENTER_DISPLAY	SAP Landscape Transformation work center - show
SAP_BTP_NWBC10_10_STD	SAP LT standard
SAP_BTP_NWBC30_10_STD	SAP LT standard
SAP_LT_PORTFOLIO_DISPLAY	SAP Landscape Transformation work center - portfolio only
SAP_LT_WORKCENTER	SAP Landscape Transformation work center
SAP_LT_WORKCENTER_DISPLAY	SAP Landscape Transformation work center - show

SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_DMIS_SLOP_CMIS	SAP SLOP Client Migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4
SAP_DMIS_SLOP_SHELL	SAP Landscape Transformation Shell Creation
SAP_LT_ANALYSIS_EXECUTION	SAP Landscape Transformation analysis execution and evaluation
SAP_LT_ANALYSIS_EXECUTION	SAP Landscape Transformation analysis execution and evaluation
SAP_LT_PORTFOLIO_DEVELOPER	SAP Landscape Transformation portfolio developer
SAP_DAL_ADMIN_LTS	Technically required

The add-on DMIS_2011 includes the following composite roles for the SAP Solution Manager system.

- SAP_LT_MASTER (All authorizations for SAP Landscape Transformation)

Contains the authorizations that are assigned to the following roles:

Contained Single Roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CMIS	SAP SLOP client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP add. authorizations for client transfer release 700
SAP_LT_ANALYSIS_EXECUTION	SAP Landscape Transformation analysis execution and evaluation
SAP_LT_WORKCENTER	SAP Landscape Transformation work center
SAP_SLOP_MASTER	SAP SLOP - Master user
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4

- SAP_LT_BUSINESS_EXPERT (SAP Landscape Transformation Business Expert)

Contains the authorizations that are assigned to the following roles:

Contained Single Roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality

SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_LT_ANALYSIS_EXECUTION	SAP Landscape Transformation analysis execution and evaluation
SAP_LT_WORKCENTER	SAP Landscape Transformation work center
SAP_SLOP_USER	SAP SLOP - Standard user for execution
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4

- SAP_LT_TECH_EXECUTION_EXPERT (SAP Landscape Transformation Technical Execution Expert)

Contains the authorizations that are assigned to the following roles:

Contained Single Roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_LT_ANALYSIS_EXECUTION	SAP Landscape Transformation analysis execution and evaluation
SAP_LT_WORKCENTER	SAP Landscape Transformation work center
SAP_SLOP_PROJECT_LEAD	SAP SLOP - Standard project lead user
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4

- SAP_LT_TECH_EXECUTION_USER (SAP Landscape Transformation Technical Execution User)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis Release 700
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_LT_ANALYSIS_EXECUTION	SAP Landscape Transformation analysis execution and evaluation
SAP_LT_WORKCENTER_DISPLAY	SAP Landscape Transformation work center - show
SAP_SLOP_USER	SAP SLOP - Standard user for execution
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1

SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4

- SAP_LT_SHOW (SAP Landscape Transformation Guest)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_LT_WORKCENTER_DISPLAY	SAP Landscape Transformation work center - show
SAP_SLOP_DISPLAY_USER	SAP SLOP - Standard user only for display

Note:

Some of the single roles such as SAP_DMIS_SLOP_APPL1 do not have authorizations. These roles are placeholders for any new authorizations for SAP LT that may be required in the future.

SAP NetWeaver Business Client

To run SAP Landscape Transformation 2.0, 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. Web browsers do not support this logout feature. For example if you use a web browser to access the work center, there is no option to logout. 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.

To use all functions and features you have to assign the role *SAP_BTP_NWBC30_10_STD* to all users who interact with the Landscape Transformation work center.

Project and Roadmaps in SAP Solution Manager

Authorizations for working with projects and roadmaps in SAP Solution Manager are required. Assign the SAP standard role **SAP_SOL_PROJ_ADMIN_ALL** to the relevant users.

User Registration

In addition to the authorization concept, SAP Landscape Transformation has a specific user registration feature. Business experts, technical execution users, and technical execution experts need not only the required authorizations for their respective role, but must also be registered for the SAP Landscape Transformation project they want to work with. This ensures that users can execute functions only in relation to the projects they are assigned to.

Only a project lead can register new members to the projects they have created. A project lead must be a business expert or a technical execution expert.

Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookies, 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](#).



Network and Communication Security

Access to all systems in an SAP Landscape Transformation system landscape takes place exclusively through RFC connections. For more information about security issues in connection with RFC, The usage of Secure Network Communication is recommended. For more information see the [RFC/ICF Security Guide](#).

Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For SAP LT 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](#).

For more information about ICF security, see the [RFC/ICF Security Guide](#).



Communication Destinations

Use

SAP Landscape Transformation does not come with fixed destinations or user names. The following destinations need to be created:

For transformation solutions that do not involve the transfer of data between systems:

- A destination from the control system to participating execution system needs to be created in the control system.
- Users in RFC destinations need to be of type dialog – and require authorizations specified by one of the following composite roles:
 - SAP_LT_RFC_USER - for SAP basis releases < 700
 - SAP Landscape Transformation RFC User - for all solutions

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorizations 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorizations 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorizations 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorizations 4

- SAP_LT_RFC_USER_700 - for SAP basis releases 700 and higher
SAP Landscape Transformation RFC User - for all solutions

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4

- SAP_LT_RFC_USER_ANA (SAP Landscape Transformation RFC User - for Analysis)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_ANA_700 (SAP Landscape Transformation RFC User - for Analysis)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
------------------------	-------------

SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CCDEL (SAP Landscape Transformation RFC User - for CCode Deletion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_CCDEL	SAP SLOP specific authorizations for company code deletion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CCDEL_700 (SAP Landscape Transformation RFC User - for CCode Deletion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CMIS (SAP Landscape Transformation RFC user - for Client transfer)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CMIS_700 (SAP Landscape Transformation RFC user - for Client transfer)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_COA (SAP Landscape Transformation RFC User - for COA Conversion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP- Basis authorizations for CWB functionality
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_COA_700 (SAP Landscape Transformation RFC User - for COA Conversion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

For transformation solutions that involve the transfer of data between systems:

- Used RFC destinations need to be defined by SAP Landscape Transformation RFC Management for each transformation solution – as destinations need to follow a naming convention that allows synchronization of destination definitions across different systems.
- 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 (use of destination NONE is NOT possible).
- 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. Based on the destination definition in the control system, the required destinations are automatically created by SAP LT RFC Management for each transformation solution.
- Users in RFC destinations need to be of type Communication / CPIC – and require authorizations specified by one of the following composite roles:
 - SAP_LT_RFC_USER (SAP Landscape Transformation RFC User - for all solutions)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations

SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorizations 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorizations 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorizations 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorizations 4

- SAP_LT_RFC_USER_700 (SAP Landscape Transformation RFC User - for all solutions)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user
SAP_DMIS_SLOP_APPL1	SAP SLOP Additional authorization 1
SAP_DMIS_SLOP_APPL2	SAP SLOP Additional authorization 2
SAP_DMIS_SLOP_APPL3	SAP SLOP Additional authorization 3
SAP_DMIS_SLOP_APPL4	SAP SLOP Additional authorization 4

- SAP_LT_RFC_USER_ANA (SAP Landscape Transformation RFC User - for Analysis)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_ANA_700 (SAP Landscape Transformation RFC User - for Analysis)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release. 700
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CCDEL (SAP Landscape Transformation RFC User - for CCode Deletion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CCDEL_700 (SAP Landscape Transformation RFC User - for CCode Deletion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CCDEL	SAP SLOP Specific authorizations for company code deletion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CMIS (SAP Landscape Transformation RFC user - for client transfer)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_CMIS_700 (SAP Landscape Transformation RFC user - for client transfer)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_CMIS	SAP SLOP Client migration - standard authorizations
SAP_DMIS_SLOP_CMIS_700	SAP SLOP Add. authorizations for client transfer release 700
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_COA (SAP Landscape Transformation RFC User - for COA Conversion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

- SAP_LT_RFC_USER_COA_700 (SAP Landscape Transformation RFC User - for COA Conversion)

Contains the authorizations that are assigned to the following roles:

Contained single roles	Description
SAP_DMIS_SLOP_BASIS	SAP DMIS SLOP - Basis authorizations for CWB functionality
SAP_DMIS_SLOP_BASIS_700	SAP SLOP Add. authorizations for Basis release 700
SAP_DMIS_SLOP_COA	SAP SLOP Specific authorizations for COA conversion
SAP_SLOP_RFC_USER	SAP SLOP - Standard RFC user

If the destinations are distributed and synchronized using the RFC management provided by SAP Landscape Transformation (as it is required for transformations solutions that involve the transfer of data between two systems, such as a client transfer), the destinations described above are created automatically and cannot be changed by standard RFC management.



Data Storage Security

Use

SAP Landscape Transformation does not create or store any sensitive data even temporarily in the control or central systems. However, during data selection, SAP Landscape Transformation extracts data relevant for migration from the application tables of the sender system and stores it separately in a cluster format. If any data transformation is necessary then this is applied on the cluster data, which is later transferred to the receiver system. This data is not accessible to the SAP Landscape Transformation dialog user. However, the data protection depends on the sender system being marked as a production client, or by restricting access to the report RSINDX00, which has administrative authorizations.

You can access the data stored in the SAP Landscape Transformation data cluster with the transaction DTLMON. In this transaction, you must specify the mass transfer ID and the access plan for the current package. The system displays a new screen where you can access information about the data volume for every migration object (on the *Runtime Information* tab page).

By default, SAP Landscape Transformation copies data as it is from the sender system to the receiver system depending upon the portfolio item selected. You can find more information about the available portfolio items in the SAP Landscape Transformation master guide. You transfer data in SAP Landscape Transformation using RFC which allows for a high level of security.



Trace and Log Files

Use

SAP Landscape Transformation does not create any trace files. However, SAP Landscape Transformation 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 process monitor for SAP Landscape Transformation.