Role and User Distribution to the SAP System

SAP Enterprise Portal 6.0 SP2

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

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

Contents

Role and User Distribution to the SAP System

SAP Enterprise Portal provides you with broad and easy-to-use functions for the creation and administration of roles and users.

In order to be able to access connected SAP systems with the roles managed in the portal, you must transfer these role definitions and user assignments to the SAP systems. For this distribution process, a component in the portal is available, which allows you to distribute the portal roles and user assignments to the SAP system.

Data on the following services can be transferred from SAP Enterprise Portal to the SAP system:

- Transactions
- Non-transactional data (for example, TADIR services or RFC-enabled function modules) in the form of authorization trace IDs

On the SAP system side, transaction WP3R is available. This allows you to assign a corresponding role in the SAP system to users and their assigned portal roles. The corresponding role (authorization role) contains the authorizations that are required to perform certain services, for example, transactions, from within the portal.

Prerequisites

The functions necessary for subsequent processing of the portal roles in the SAP system are available if you import SAP Enterprise Portal Plug-In 6.0 to your SAP systems.

Constraints

- Release 4.0

  The portal data can only be displayed. You can neither create authorization roles nor assign roles to users.

- Release 4.5

  You cannot assign roles to users if the central user administration is used with global role assignment and a central system of Release 4.5.

- Release 6.20

  Support for default authorization values for services is provided through support packages. You can find out the current status in SAP Note **640759**.

- Enterprise Portal Plug-In < 6.0

  If you use an Enterprise Portal Plug-In < 6.0 and your Basis release is earlier than 6.20, the system does not support the transfer of authorization trace IDs.

The documentation on role and user distribution is divided into the following sections:

Role Distribution Process

Purpose

Role and user assignments that are created and managed in SAP Enterprise Portal have no authorizations in the SAP system. A user is only granted authorization to execute services, for example, transactions and BSP applications, in a SAP system from the portal once the portal roles have been transferred to the corresponding SAP system and the corresponding authorization role has been correctly assigned. In the portal role, these are iViews containing accesses to services in the backend system.

You cannot transfer roles from the Enterprise Portal to the SAP system on a one-to-one basis because the roles have different definitions. Instead, authorization roles (see Maintenance of Authorization Roles [Seite 18]) that only contain objects that are relevant for the SAP system are created in the SAP system. The authorization roles in the SAP system are single roles with menu and authorization data.

Process Flow

The roles defined on the portal side must be transferred to the connected SAP systems. The distribution process has two steps:

1. **In the portal**: Distribute the role definitions and user assignments to the SAP system that is responsible for role maintenance within the system landscape.

   You can call the distribution function in the administrator role with *System Administration → Permissions → R/3 Permissions.* When you transfer the roles, the entries relevant for authorization maintenance in the SAP system are filtered out in the portal role. You can transfer transactions and non-transactional services to the SAP system. All other objects are ignored.

   Note that you first distribute the portal roles to the SAP system and then distribute the role-user assignments.

2. **In the SAP system**: Manual follow-up processing of the transferred roles using transaction WP3R.

   In the SAP system, you must create an authorization role per portal role and per logical system. You can create more than one authorization role per portal role and per logical system, depending on how many authorization profile versions you require.

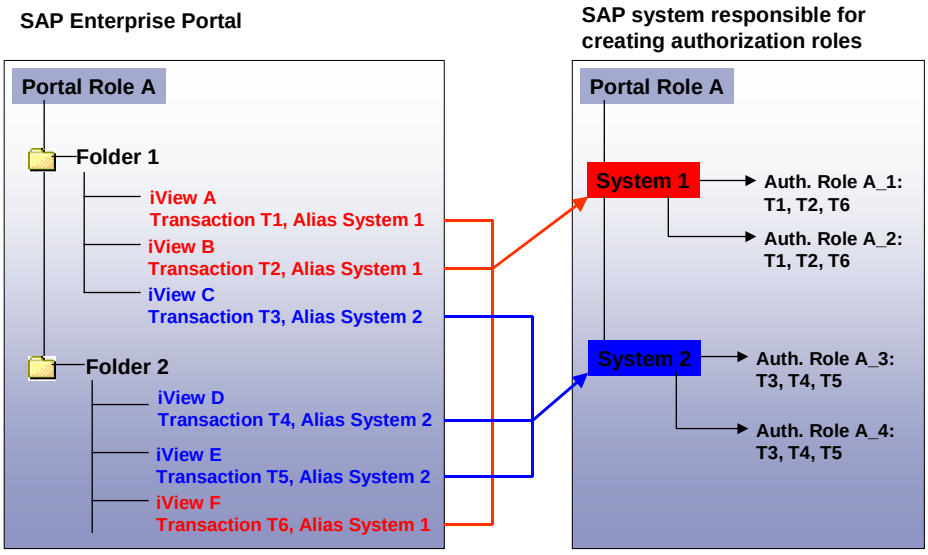
   Afterwards, you assign the authorization roles to the SAP users.

   The process requires manual follow-up processing since, in contrast to roles in the SAP system, portal roles do not recognize the division into responsible organizational units (such as company codes and plants) and therefore cannot supply the authorization checks connected with the transaction with data.

Example

The following graphic shows how the portal definition of a role is assigned to the SAP system:



In a portal role, a search mechanism determines the iViews containing transaction codes for a certain logical system. An alias name is used to determine the logical system in which the transaction codes contained in the iViews should be distributed together with the corresponding portal role names. For more information about the search mechanism see Transferring Role Data [Seite 10].

At least one authorization role must be created for each logical system in the SAP system.

Transferring Role Data and Assignments to the SAP System

SAP Enterprise Portal offers a function that allows you to transfer the role data and assignments that you create and maintain in the portal to connected SAP systems.

The following data is filtered out of the portal roles and transferred:

- Contained transaction code, where iViews are the only objects in a portal role that may access SAP transactions.
- Authorization trace IDs: These are non-transactional objects for which authorization in the backend system is also required when an iView is launched in the portal. In the SAP system, a trace ID is generated for each iView. For the trace IDs, you must create certain ABAP authorizations in the backend system, for example, to call RFC-enabled function modules. SAP delivers the necessary authorization objects for the trace IDs in advance.

You can find out how to proceed with the data transfer in:

Creating Systems for Role Distribution

Use

You have to create a system in the portal system landscape and to connect it with the SAP system to which the role and user assignments should be transferred. This is usually a SAP system that is responsible for role maintenance and user assignment. For more information, see System Landscape [Seite 14].

You can also distribute portal roles to one SAP system and the user assignments to another system, depending on how your SAP system landscape is designed.

Procedure

1. Launch the System Landscape Editor [Extern] with *System Administration* → *System Configuration* → *System*.
2. Create a system that is connected to a SAP system. You can find out how to create this connection in Creating a System [Extern] and Editing SAP System Properties [Extern].
3. Create an alias for the system, for example *RoleMaintenance*. You can find out how to create a system alias under Maintaining a System Alias List [Extern].

   Use these alias names when you distribute roles. For more information see Transferring Role Data [Seite 10].

For more information, see SAP Help Portal on **`help.sap.com/ep`** → *Administration Guide*.

In the Administration Guide you also find the external links mentioned above:

Link	**Path**
System Landscape Editor	*SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System* Administration → *System Landscape* → *System Landscape Editor.*
Creating a System	*SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System* Administration → *System Landscape* → *System Landscape Editor -> Creating a System.*
Editing SAP System Properties	*SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System* Administration → *System Landscape* → *System Landscape Editor* → *Editing System Properties* → *Editing SAP System Properties.*
Maintaining a System Alias List	*SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System* Administration → *System Landscape* → *System Landscape Editor* → *Maintaining a System Alias List.*

Assigning Logical Systems

Use

The SAP system landscape has not been assigned to the portal system landscape. This means that neither the names of the logical SAP systems nor their responsibilities have been assigned to the portal.

In table WP3ROLESYS which is in the SAP system landscape responsible for role maintenance you define the logical systems for which this system is responsible for role maintenance. For more information, see Mapping System Responsibilities [Seite 15]. The information in table WP3ROLESYS must be assigned in the portal system landscape. Before SAP Enterprise Portal transfers role data to the SAP system that is responsible for role maintenance, this SAP system informs the portal which logical systems it is responsible for.

Using the logical system name the portal can read the data that is relevant for the role transfer from the portal roles and transfer it to the system responsible for role maintenance. The logical systems must be assigned to the portal systems within the portal system landscape.

You **cannot** find out which systems are responsible for user assignments in table WP3ROLESYS. These systems are automatically derived from the SAP system landscape using a certain algorithm. To learn how to find these systems, see Transferring User Assignments [Seite 12].

Prerequisites

- You set up an SAP system landscape and maintain the responsibilities in table WP3ROLESYS. For more information, see System Landscape [Seite 14] and Adjusting System Responsibilities [Seite 15].
- Create a portal system landscape. To do this, read System Landscape [Extern] and System Landscape Editor [Extern]

In the SAP Enterprise Portal Administration Guide you find the external links mentioned above. You will find the Administration Guide on the SAP Help Portal on **`help.sap.com/ep`** → *Administration Guide*.

Link	Path
System Landscape	*SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System* Administration → *System Landscape*
System Landscape Editor	*SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System* Administration → *System Landscape* → *System Landscape Editor.*

Procedure

1. In the SAP system that is responsible for role maintenance, check in table WP3ROLESYS which logical system names must be assigned to the portal.
2. Consider which portal systems correspond to these logical system names or which portal systems refer to these logical systems in your portal system landscape.
3. Launch and edit the relevant portal systems with *System Administration* → *System Configuration* → *System*.
4. Set property category „Connector“ in the dropdown list for each system.
5. Define all the properties necessary to connect to a SAP system, for example *Logical System Name*, *Client*, *Message Server*, *R/3 Name*.

Transferring Role Data

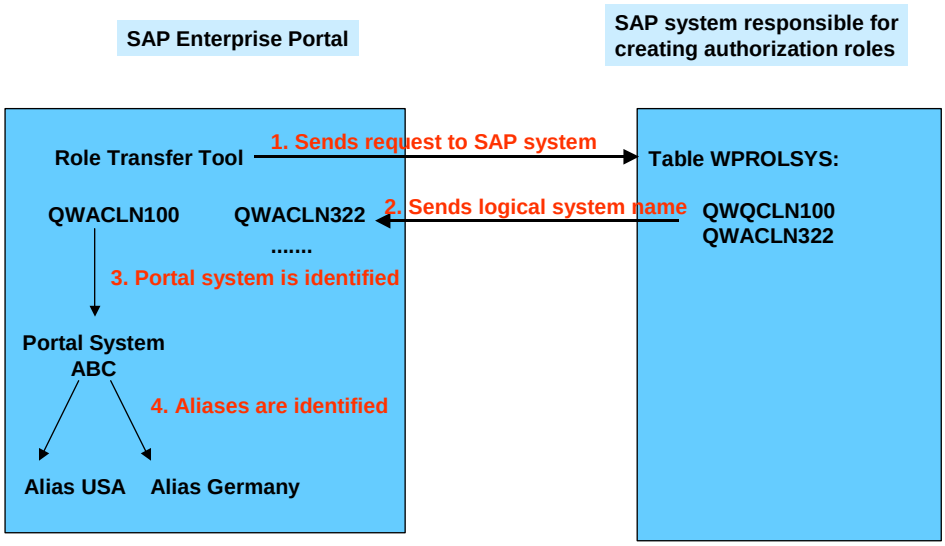
Use

SAP Enterprise Portal offers you a function for transferring the portal roles defined in the Enterprise Portal to connected SAP systems. Usually, you transfer the roles to a particular SAP system, which is responsible for creating and maintaining the authorization roles within the SAP system landscape. For more information, see System Landscape [Seite 14].

Procedure

1. In SAP Enterprise Portal choose *System Administration* → *Permissions* → *R/3 Permissions.*
2. To transfer the portal roles to the SAP system, select *Transfer Role Permissions* and choose *Next*.
3. On the **Transfer Role Permissions** screen, choose the system to which you want to transfer the roles from the dropdown list. The alias names are displayed in the dropdown list. Select the alias names you maintained for the system in which the roles are distributed. Read also Creating Systems for Role Distribution [Seite 8].

   The following graphic shows the search mechanism based on it:



   The portal first uses an RFC module to access table WP3ROLESYS, where the system responsibilities for role maintenance are entered (see step 1 in the graphic). The logical system names are returned to the portal and displayed in a list (see step 2). The portal finds the corresponding portal systems using the logical system names (see step 3). The corresponding aliases are found from the portal systems (see step 4). If no portal system is found for a logical system or no alias is maintained for a portal system, there is a warning and a corresponding status message.

4. Decide which roles you want to transfer. You have the following options:
   - Option one: Select from transferred roles

- Option two: Transfer all transferred roles again
- Option three: Select from complete set of portal roles
- Option four: Transfer all portal roles

If you choose options one or three, you come to a screen, on which you can select the roles that you want to transfer. Select the entries and choose *Next*. A screen appears, on which you can check your transfer settings.

If you choose options two or four, you go directly to the screen on which you can check your transfer settings.

If you select *Include R/3 Authorization Trace IDs*, the system automatically generates trace IDs in the SAP system for the iViews contained in the portal role. For more information about trace IDs, see Roles and User Distribution to the SAP System [Seite 1].

5. Check all your settings for the role transfer. A name is proposed for the report that performs the transfer. You can overwrite this proposal.

   You can also save your transfer settings under a name and then reuse them. For more information, see the section on *Transfer Process with Predefined Settings*.

6. Choose *Finish*. This starts the transfer of the roles.

   In this process, the portal checks which of the iViews contained in the roles contain the alias names identified in step 3. All the iViews containing the relevant alias names are selected. The transaction names entered in the iViews are transferred to the SAP system together with the portal role names.

   An iView that refers to a transaction in a SAP system always contains an alias name as property.

7. A further screen appears which displays the log messages for the role transfer report. With *Interrupt Transfer* you can interrupt the transfer at this location.

   You can look at the log files for each transfer report again at any time.

   - To do so, select the option *Display Report Overview* on the initial page of the role transfer and choose *Next*.
   - Decide if you want to display the log files for the role transfer or for user assignments.
   - In the list, select a transfer report and choose *Display Report*.

Transfer Process with Predefined Settings

You can also save your settings under a given name. To do this, choose *Save as predefined transfer settings* on the screen for checking your settings and enter a name.

The advantage of this is that you can reuse the settings instead of having to enter all the information again for the next transfer run.

If you use predefined settings, steps two to six are not relevant, You only work through step one and start the transfer there, by selecting the name of your predefined settings under **Predefined Transfer Settings** and starting the transfer. You can then view the log files, as described in step seven.

Transferring User Assignments

Use

SAP Enterprise Portal offers you a function for distributing defined user assignments to connected SAP systems. You usually distribute roles to the system that is also responsible for role maintenance.

You must distribute the associated roles before you distribute the user assignments.

Prerequisites

In order for the distribution of the user assignments to work correctly, the user IDs in the portal must be identical to those in the SAP system:

- If you already have identical IDs, you do not need to do anything else.
- If you have different user IDs, you must map the portal users to the SAP users. For more information, see User Mapping [Extern].

The mapped user is always transferred when you transfer the user assignment data.

Another way to make sure that you have identical user IDs is to use the SAP system as the data source for your user data. For more information see Defining a SAP System as a Data Source [Extern].

In the SAP Enterprise Portal Administration Guide you find the external links mentioned above. You will find the Administration Guide on the SAP Help Portal on **`help.sap.com/ep`** → *Administration Guide*.

Link	Path
User Mapping	*Administration Guide → Portal Platform → User Administration → User Mapping.*
Defining a SAP system as a Data Source	*Administration Guide → Portal Platform → User Management Configuration → Configuration of Data Sources Used for User Management → Defining a SAP system as a Data Source.*

Procedure

1. In SAP Enterprise Portal choose *System Administration → Permissions → R/3 Permissions.*
2. To transfer the portal roles to the SAP system, select *Transfer User Assignment* and choose *Next*.
3. On the **Transfer User Assignment** screen, choose the system to which you want to transfer the role-user assignments from the dropdown list. The alias names are displayed in the dropdown list. Select the alias names you maintained for the system in which the assignments are transferred. Also read Creating Systems for Role Distribution [Seite 8].

   The list of logical systems for which the system you are transferring the assignments to is responsible appears. In contrast to the role transfer, the system does not analyze table WP3ROLESYS to display this list. This data is derived automatically from the SAP system landscape. For more information, see System Landscape [Seite 14]. There is an error message if the logical systems for user assignment are not assigned to the portal. You can find out how the logical systems are assigned to the portal system landscape by reading Assigning Logical Systems [Seite 9].

4. Specify which user assignments you want to transfer. There are two ways to do this:
   - Option one: From a list of roles that have already been transferred, you can choose those for which the system is to transfer the user assignment.
   - Option two: You transfer the user assignments for all roles that have already been transferred.

   If you choose option one, a screen appears on which you can select the roles whose user assignment you want to transfer. Select the entries and choose *Next*. A screen appears, on which you can check your transfer settings.

   If you choose option two, you go directly to the screen on which you can check your transfer settings.
5. Check your settings. A name is proposed for the report that performs the transfer. You can overwrite this proposal.

   You can also save your transfer settings under a name and then reuse them. For more information, see the section on *Transfer Process with Predefined Settings*.
6. Choose *Finish*. This starts the distribution of the user assignments.
7. A further screen appears which displays the log messages for the role transfer report. With *Interrupt Transfer* you can interrupt the transfer at this location.

   You can look at the log files for each transfer report again at any time.
   - To do so, select *Display report overview* on the initial page **Transfer Role Information to R/3** and choose *Next*.
   - Decide if you want to display the log files for the role transfer or for user assignments.
   - In the list, select a transfer report and choose *Display Report*.

Transfer Process with Predefined Settings

You can also save your settings under a given name. To do this, choose *Save as predefined transfer settings* on the screen for checking your settings and enter a name.

The advantage of this is that you can reuse the settings instead of having to enter all the information again for the next transfer run.

If you use predefined settings, steps two to six are not relevant, You only work through step one and start the transfer there, by selecting the name of your predefined settings under *Predefined Transfer Settings* and starting the transfer. You can then view the log files, as described in step seven.

Follow-up Processing for Portal Roles in the SAP System

The roles and user data transferred from the portal must be applied to authorization roles and the corresponding assignments in the relevant SAP systems. This process cannot be fully automated; follow-up processing must be performed manually.

The following sections explain how to manage and maintain authorization roles and their assignments in an SAP system.

- Requirements [Seite 14]
- Maintenance of Authorization Roles [Seite 18]
- Assignment of Authorization Roles [Seite 25]
- Cleaning up Data [Seite 29]

Prerequisites

The sections of this chapter explain the elementary requirements necessary in order to create authorization roles from portal roles.

- System Landscape [Seite 14]
- Adjusting System Responsibilities [Seite 15]
- Authorizations [Seite 17]

System Landscape

Background

To define the system responsibilities within your SAP system landscape, you must enter the system responsible for role maintenance in table WP3ROLESYS. For more information, see Mapping System Responsibilities [Seite 15].

Note that responsibility for user assignment is not defined using table WP3ROLESYS. This data is derived from the SAP system landscape and you do not have to maintain it manually.

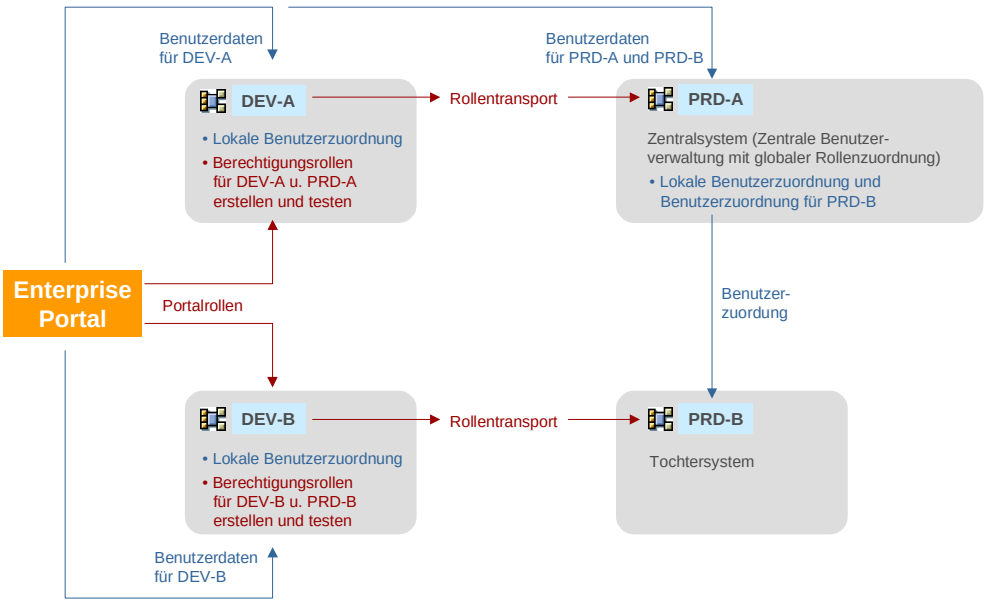
Afterwards, you must modify the SAP system landscape to suit the portal system landscape. For more information, see Assigning Logical Systems [Seite 9].

Example

The following example shows how roles and user data are assigned to SAP Enterprise Portal and two connected SAP system landscapes.

In this case the SAP system landscapes consist of a development system (DEV-A, DEV-B) and a production system (PRD-A, PRD-B) each. Production system PRD-A performs the functions of a central user administration with global role assignment.

The following graphic shows the system landscape and functions that the individual systems perform for role and user administration.



The portal defines roles with services in system landscapes A and B. The corresponding authorization roles are created and tested in development systems DEV-A and DEV-B and transported to the relevant subsequent production systems with the role transport.

The data for user assignment is transferred from the portal to the relevant systems (see Mapping System Responsibilities [Seite 15]) (DEV-A, PRD-A and DEV-B). System PRD-B is not responsible for user assignment. It is linked to the central user administration of system PRD-A. Central system PRD-A therefore also receives user data for system PRD-B as well as for itself.

The system landscape described above is a complex example. A landscape consisting of a single system is also possible.

Adjusting System Responsibilities

Use

Before the Enterprise Portal transfers role data to an SAP system, the SAP system informs the portal which systems it is responsible for. The portal can then select the right data and transfer it to the system.

Table WP3ROLESYS determines responsibility for role maintenance.

Prerequisites

You have authorization to maintain the table view for WP3ROLESYS.

Procedure

To define that systems A and B in the example in the section System Landscape [Seite 14] are responsible for role maintenance:

1. Launch the table view maintenance (transaction SM30)for table WP3ROLESYS.
2. Make an entry for each system whose roles are to be maintained in the current system and set the *Role maintenance active* flag.

Example

Make the following entries for system landscapes A and B in table WP3ROLESYS:

Logical System	**Role maintenance active**
In System DEV-A	
DEV-A	x
PRD-A	x
In System DEV-B	
DEV-B	x
PRD-B	x
In System PRD-A	
No entries	
In System PRD-B	
No entries	

Result

The SAP systems tell the portal that the following are responsible for role maintenance:

- DEV-A for DEV-A and PRD-A
- PRD-A for no system
- DEV-B for DEV-B and PRD-B
- PRD-B for no system

For role assignment, the following responsibilities are transferred (this data is derived from the system landscape – you do not need to maintain is manually):

- DEV-A for DEV-A
- PRD-A for PRD-A *and* PRD-B
- DEV-B for DEV-B
- PRD-B for no system

Make sure that each transport track has only one system that is responsible for role maintenance:

An authorization role belongs to exactly one portal role and its services in a target system. If you maintain roles in multiple systems of a transport track, you cannot prevent roles with the same name from being created and an authorization role from being derived from multiple portal roles by the transport. Further system behavior is undefined in such a situation.

Authorizations

To transfer data from the portal to the SAP System, the user in the SAP System which is used by the portal must have authorization for role administration in the SAP System.

- Release 4.0: Authorization object PLOG

  OTYPE: T

  INFOTYP: 1000

  ISTAT: 1

  PPFCODE: AEND and DISP

- Release 4.5 and higher: Authorization object S_USER_AGR

  ACTVT: 02 and 03

You need the following authorizations for follow-up processing of the transferred data with Transaction WP3R:

- Authorization to execute Transaction PFCG (role maintenance)
- Authorization to execute Transaction SU01 (user administration)

To display the data with Transaction WP3R you need the following version of this authorization: "Display" (PPFCODE = DISP or ACTVT = 03).

Maintenance of Authorization Roles

Background

The following data is transferred when the role data is transferred from the portal to the SAP system:

- Names of the portal roles
- List of the services in the logical systems. The SAP system assumes the following objects under Services: Transaction names and trace IDs transferred from the portal.

This data is used to create authorization roles in the SAP system containing the necessary authorizations for using the services.

You can represent your organizational units by deriving multiple authorization roles from one portal role and adjusting the authorization data appropriately in the authorization roles.

The following sections explain how to maintain the authorization data:

Working with Transaction WP3R

Use

Transaction WP3R performs all the functions for the maintenance and follow-up processing of the roles and user assignments that were transferred from the portal.

Procedure

To maintain the role and user data:

1. Start transaction WP3R.
2. Choose one of these options:

Maintaining Authorization Roles	Assigning Authorization Roles To Users
Select the *Maintain Authorization Roles* function and choose *Execute*. A report is executed, which displays all available portal roles hierarchically. For each portal role, the following information is displayed: • The logical system for which there are services • Existing authorization roles with their inheritance relationships	Select the *Assign Authorization Roles To Users* function and choose *Execute*. A report is executed, which displays the following information for each user hierarchically: • Portal roles assigned to the user in the portal • Logical systems whose services are accessed by the portal role • Derived authorization roles
For more information, see Creating Authorization Roles [Seite 20].	For more information see Assigning Roles [Seite 26].

3. In the general settings for transaction WP3R, you can define whether the portal roles appear hierarchically according to the hierarchy in the portal catalog. In addition, you can define whether only lines with messages appear.

Status Display and Icons

Within the *Maintain Authorization Roles* and *Assign Authorization Roles To Users* functions, there is a status display next to each line, which contains information about the current line and all other lines below it. This also ensures that warnings and error messages from branches that are not expanded are also displayed.

A message window is opened when you click the status display symbol. There are the following status displays:

	No message exists
	Information message exists
	Warning messages exist
	Error messages exist

Some of the functions can be called from the icon on the line to be edited as well as from the menu.

	Create/convert role
	Deleting Authorization Roles
	Display services
	Compare services
	Maintain authorization data

You can also find this list by choosing *Utilities* → *Color key*.

Creating Authorization Roles

Use

You can create a new authorization role in the SAP system with the *Create/Convert Role* function.

Prerequisites

To monitor and maintain the data transferred from the portal to the SAP system you need role administration authorization (see Authorizations [Seite 17]).

Procedure

To create a new authorization role:

1. Start transaction WP3R.

   The initial screen for role administration, *Follow-Up Processes for Portal Roles*, appears.

2. On the initial screen, select *Maintain Authorization Roles* and run the program.

   A report is displayed containing all portal roles and the authorization roles associated with them. Roles transferred from the portal are highlighted in blue. The warning icon allows you to identify that there are no authorization roles for these roles.

   If a role is highlighted in red, it has been deleted in the portal.

3. To find out which services there are for a role, expand the structure of the relevant role, select a logical system, and choose *Goto* → *Service list* or  .

   If SAP Enterprise Portal has transferred services that are not supported in the current system, these are displayed in a separate section of the service list and ignored when the services are transferred to the authorization role.

4. To close the window with the service list, choose *Continue*.

5. Click the logical system and choose *Authorization role* → *Create/Convert* or choose the  icon next to the logical system.

   The system asks for the name of the new role. If you enter a name for which there is no role to date, the system creates a new one. You can also create more than one authorization role per logical system, depending on how many authorization versions you require.

   If you enter the name of an existing role, the system informs you that you can convert this role to an authorization role. The conversion can only take place if you enter the name of a root single role (not a derived role or a composite role).

   When converting an existing role to an authorization role, the system assumes that the structure of the role is defined forthwith through the enterprise portal and role assignment is only assigned through the enterprise portal. During conversion, a dialog box points out the consequences.

   The services of the portal role are immediately transferred to the menu structure of the new role. You can also use the *Create/Convert* function for authorization roles. It can be used to create derived authorization roles.

A warning is given if no authorization roles were yet created for the services of a portal role for a logical system.

Generating Authorizations

Use

Maintaining the authorization data includes completing the proposed authorization values entered by the system for the SAP transactions and trace IDs contained in the portal role.

Prerequisites

- To maintain the data transferred from the portal to the SAP system you need role administration authorization (see Authorizations [Seite 17]).
- You are on the Role Administration screen *Follow-Up Processes for Portal Roles* and have chosen the option *Maintain Authorization Roles*.

Procedure

To maintain the authorization data:

1. Click an existing authorization role and choose *Authorization role* → *Merge and maintain authorizations* or choose the  icon next to the authorization role.

   The screen for maintaining the role authorizations is opened. The proposed values are derived from the transactions and services in the menu structure.

2. Check and complete the authorization data.
3. Generate the authorization profile by choosing *Generate*  .
4. Return to the screen for Role Administration.

   You can also call the screen for maintaining authorization data with transaction *PFCG*. However, the data needed to maintain the authorization roles does not appear here. You should therefore **always** start maintenance of the authorization roles from transaction *WP3R*.

For more information about the general SAP authorization concept and how to generate authorizations, see the SAP Help Portal: *SAPNetWeaver* → *SAP Web Application Server.* In the SAP Library, choose *SAP NetWeaver Components* → *SAP Web Application Server* → *Security* → *Users and Roles.*

Adjusting Services

Use

If the services of a portal role for which an authorization role was already created in the SAP system are changed in the portal, you must adjust the definitions of the portal and authorization roles.

Prerequisites

- To maintain the data tranferred from the portal to the SAP system you need role administration authorization (see Authorizations [Seite 17]).
- You are on the Role Administration screen *Follow-Up Processes for Portal Roles* and have chosen the option *Maintain Authorization Roles*.

Procedure

If you change the services of a portal role for which authorization roles were already created in the portal, these authorization roles are marked with a warning  . To adjust the services of an authorization role to those of a changed portal role:

1. Place the cursor on an authorization role and choose *Goto* → *Service compare* or choose the  icon next to the authorization role.

   The services of the authorization role are compared with those of the portal role.

2. To copy the changed services to the menu structure of the authorization roles, choose *Authorization role* → *Update*.

   You can either execute the function for a single authorization role by placing the cursor on this role or select multiple authorization roles with the editing functions before executing the function.

   You may also have marked other objects when you perform this function. The function ignores these objects. For example you can select the entire hierarchy to adjust all the authorization roles.

3. After adjusting the authorization roles, you must check the authorization data again and adjust it if required. For more information, see Maintaining Authorization Data [Seite 21].

Deleting Authorization Roles

Use

When deleting an authorization role, the system offers to either remove only the connection between the authorization role and the portal role, or to delete the authorization role completely.

Prerequisites

- To maintain the data copied from the portal to the SAP system you need role administration authorization (see Authorizations [Seite 17]).
- You are on the Role Administration screen *Follow-Up Processes for Portal Roles* and have chosen the option *Maintain Authorization Roles*.

Procedure

To delete an authorization role:

1. Place your cursor on an authorization role.
2. Choose *Authorization role* → *Delete* or choose the icon next to the authorization role.

   A dialog box appears, in which you state, whether you want to remove only the connection between the authorization role and the portal role, or to delete the authorization role completely.
3. If you want to remove the connection, choose *Remove* in the dialog box. If you want to delete the authorization role, choose *Delete*.

   You should only delete authorization roles using this maintenance transaction. If you delete roles using other methods, the administration data needed for assigning portal roles is not deleted.

   You cannot use the deletion function for more than one role simultaneously.

Transporting Roles to other Target Systems

Depending on the structure of your system landscape, you have to transport the authorization roles created and maintained in one system to the other systems and make them available there (see System Landscape [Seite 14]). The system automatically copies the roles with customizing requests.

You have to enter a customizing request for all changes to authorization roles. This ensures that the roles as well as the administration data are distributed in the target system of the transport.

If a role transport is not required, you can deactivate the field for the automatic transport request on the initial screen for role distribution, for example if the role is created and used in the same system.

You can also trigger the transport manually by choosing *Authorization role* → *Transport.* This is necessary for example if you temporarily deactivated the field for automatic transport requests for test purposes and later decide you want to copy your changes to the target systems after all.

Prerequisites

- To maintain the data copied from the portal to the SAP system you need role administration authorization (see Authorizations [Seite 17]).
- You are on the Role Administration screen *Follow-Up Processes for Portal Roles* and have chosen the option *Maintain Authorization Roles*.

Procedure

To transport roles to another system:

1. Select one or more roles.
2. Choose *Authorization role* → *Transport*.

   The selected roles are transported.

   You can also call the authorization role transport with transaction *PFCG* under *Download/Upload*. The administration data of the portal roles are not copied if you trigger the transport with this transaction.

   You should therefore always start the transport from transaction *WP3R*.

   Roles are always transported together with their profiles. The option to suppress the profile transport (table PRGN_CUST, entry PROFILE_TRANSPORT) is ignored.

Checking Role Transports

Use

Transaction WP3R can be used to check whether roles were correctly transported to target systems lying on the transport track. You can display and check the role and user data by

calling the transaction in a target system. However, you cannot make any changes in this system using transaction WP3R.

Prerequisites

- To maintain the data copied from the portal to the SAP system you need role administration authorization (see Authorizations [Seite 17]).
- You are on the Role Administration screen *Follow-Up Processes for Portal Roles* and have chosen the option *Maintain Authorization Roles*.

Procedure

To check the role transport, start transaction WP3R in a target system.

You cannot execute any operations that change the data if the system is not responsible for role maintenance in Customizing (table view WP3ROLESYS).

Assigning Authorization Roles

The assignment of roles to users is transferred with the user data to the relevant SAP systems (see System Landscape [Seite 14]). The user data contains a list of portal roles and SAP user names.

The assignments transferred from the portal must be converted on the SAP system side, that is, the authorization roles derived from the portal roles must also be assigned to the relevant users in the SAP system.

The following sections explain how to assign the authorization roles to the right users:

Prerequisites

The data created during role maintenance must exist in the role allocation system before you can assign the roles. The data might not yet exist in this system for one of the following reasons:

- The roles were created in another system and the transport requests created during role maintenance were not yet imported.

  Make sure the data is imported.

- If you are using central user administration with global role assignment, you first have to read the role definitions from the client systems.

  The initial screen of transaction WP3R then also contains the *Read roles from client systems* pushbutton. This function can only be performed correctly if all client systems can be reached synchronously.

  All the users who are to be assigned roles must first have been copied to the central user administration. If you activate central user administration or add new systems, you must first close the copy process before assigning the portal roles.

  Check the copy process with transaction SCUG: None of the systems should have status *New*.

Assigning Roles

Use

All the functions for the maintenance and follow-up processing of the roles and user assignments transferred from the portal are performed using transaction WP3R (see Working with Transaction WP3R [Seite 18]).

Prerequisites

- The role data must exist in the role assignment system (see Prerequisites [Seite 26]).
- To maintain the data transferred from the portal to the SAP system you need user administration authorization (see Authorizations [Seite 17]).

Procedure

To assign an authorization role on the SAP system side:

1. Start transaction WP3R and select the option *Assign Authorization Roles To Users* on the initial screen.

   A report is started which looks like role maintenance but which contains an additional hierarchy level containing the SAP user name. The SAP user name contains the following entries:

   - Portal roles assigned to the user in the portal
   - Logical systems whose services are accessed by the portal role
   - Derived authorization roles

   If a warning message appears in the hierarchy,

2. Each authorization role is preceded by a checkbox that shows whether the user is currently assigned to the authorization role.

   Assign the users to the corresponding authorization roles by activating the checkboxes in front of the authorization roles or by choosing *Authorization role* → *Assign*.

   You can delete the assignment by clicking the activated checkbox or by choosing *Authorization role* → *Unassign.*

3. Save the assignments you have made.

The system expects at least one authorization role to be assigned for each logical system that is assigned to a portal role. Vice versa, the system also expects you to remove all authorization roles from the assignment if the portal cancels a user's authorization for a portal role.

You can assign the roles automatically by choosing *Utilities* → *Propose Assignment*. The system automatically sets the assignments for all users displayed. This only works if there is only **one** authorization role for a portal role. You can also schedule automatic assignment as a background job. For more information, see Automatic Role Assignment in the Background [Seite 28].

However, there is very often more than one authorization role for a portal role in the same logical system. This is the case, if you require different versions of a particular authorization in the backend system and therefore you must also generate different authorization roles and the associated authorization profiles. See also Creating Authorization Roles [Seite 20].

In this case, the system cannot automatically assign the authorization role to the user. If more than one authorization role and profile are available for a user, as the administrator you decide which roles in the backend system to assign to the user and which not to assign.

If there is more than one authorization role for a portal role in a logical system, the system issues a warning so that you know that the system has not assigned an authorization role to the user and you must assign one manually.

Time-dependent role assignments are not taken into consideration. The authorization role is always assigned with a validity from the current date until December 31, 9999.

Automatic Role Assignment in the Background

On the initial screen of transaction WP3R, you can automate role assignment for the *Assign Authorization Roles* function by selecting the option *Assign Automatically and Update Immediately*.

If this option is selected, the transaction assigns and saves the role without any further interaction. Automatic assignment only works if there is only one authorization role per portal role. See also Assigning Roles [Seite 26].

Messages are output in a list and not in the message window.

This function should be used to schedule regular updates of the role assignments in the background.

If you are using central user administration with global role assignment, the background job should first execute report WP3ROLELIST_GET_CLIENT_ROLES to read the current role data of the client systems and only then execute report WP3ROLELIST.

Executing report WP3ROLELIST_GET_CLIENT_ROLES corresponds to the function *Read roles from client systems*.

Error Situations

If you are using central user administration with global role assignment, the system cannot immediately point out all errors when saving.

You should therefore check the status of user distribution regularly with Transaction *SCUL*.

Cleaning Up Data

Use

You can delete incorrect data or portal role data that you no longer need using transaction WP3R.

Typical situations where this could be necessary are:

- The portal sent data to the wrong system.
- Authorization roles were changed outside of transaction WP3R.
- Role data was not completely transferred.
- Portal roles were deleted in the portal and are no longer required in transaction WP3R.
- The portal role has no user assignment in transaction WP3R and can therefore be deleted.

Prerequisites

- To maintain the data tranferred from the portal to the SAP System you need role administration authorization (see Authorizations [Seite 17]).
- You are on the initial screen for either authorization role administration or role assignment.

Procedure

To clean up the data in the SAP System, choose *Utilities* → *Cleanup*.

You can use this function in the following ways:

- **Authorization roles**: An authorization role was assigned to a portal role, but later deleted or changed outside of transaction WP3R. This results in an error message. The function therefore removes the assignment.
- **Portal roles:**

  Portal roles that are flagged as deleted in the portal, are highlighted in red in transaction WP3R. These can now be deleted in transaction WP3R. In authorization role maintenance mode, you can delete a portal role if the authorization roles derived from this portal role have already been deleted.

  Portal roles can be deleted in role assignment mode if they no longer belong to any user role assignment. For example, this can happen if the user assignment to a portal role is transferred to the SAP system, but no corresponding user can be found in the SAP system.

  Portal roles without a user assignment appear in transaction WP3R with user name "<?>".
- **Users**: All role assignments for a user can be deleted if this user is no longer assigned to any authorization role.

You can perform this function for a number of selected entries. For technical reasons, however, you cannot always delete all the selected entries at one time. Examples of this are:

- Portal roles and the related incorrect authorization roles are selected. Initially the function cannot delete the portal roles because there are still dependent authorization roles. For this reason only the authorization roles are initially deleted. The next time the function is performed, the portal roles themselves can also be deleted.
- You can delete roles assignments with the *Utilities* → *Cleanup* function for one user. The system cannot detect that there are unnecessary portal role records caused by these deletions (displayed with the user name "<?>") until the next time transaction WP3R is started. The portal roles can only be removed now.