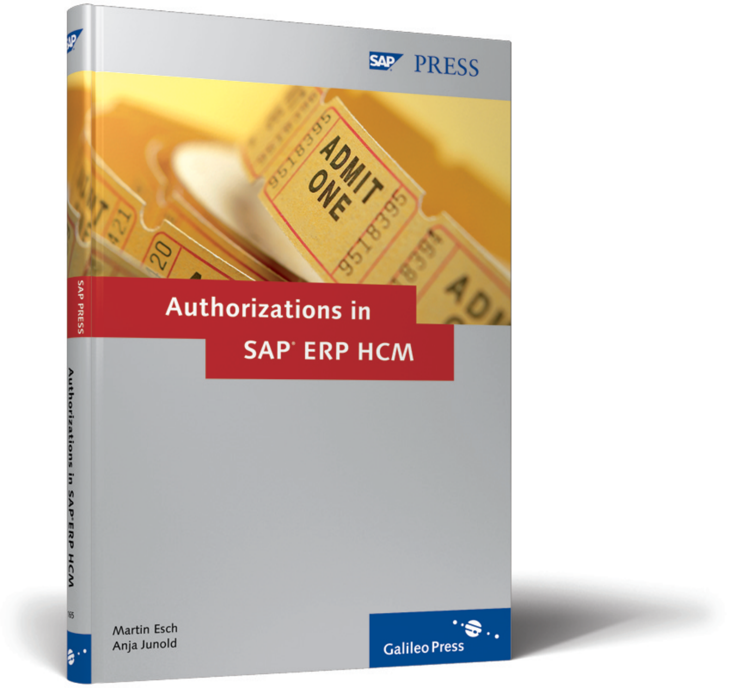
Martin Esch, Anja Junold

Authorizations in SAP® HR



www.sap-press.com

Galileo Press

Bonn • Boston

Contents at a Glance

Contents

In SAP ERP HCM, many things don't work without a structural authorization check — or only if a great deal of maintenance effort is involved. This chapter describes the benefits of structural authorizations and where you can best use them.

3 Structural Authorization Check

The structural authorization check supplements the general authorization check. It uses the arrangement and flexibility of structures in the HCM system to simplify the authorization profiles and increase their dynamics. The structural authorization check is used in three essential areas:

- Display and maintenance of objects in Organizational Management (OM)
- Display and maintenance of all other HCM objects that are stored in tables of the HRP* structure
- Organizational restrictions for the display and maintenance of personnel administration data

Only in SAP ERP HCM

A structural authorization check as it is described here exists only in SAP ERP HCM. The following sections first introduce the concept of structural authorizations in Organizational Management. After demonstrating how you can configure a structural authorization, we will describe additional fields of application. The section on the maintenance of structural authorizations ends with the description of how you can assign structural authorizations to users. Then, some specific problems are specified and, finally, we'll again focus on the extension options of the tool.

3.1 Structural Authorization Check in Organizational Management

PLOG doesn't check the content

When examining the PLOG object, it's apparent that it doesn't provide the option to exclude or permit access to certain objects. For example, if the authorization for Infotype 1000 of object type S is granted, it applies to all positions of the enterprise. The PLOG authorization object doesn't enable you to determine for which areas of the enterprise positions may be displayed or managed. But this can be done using the structural authorization check.

OM tool: evaluation path

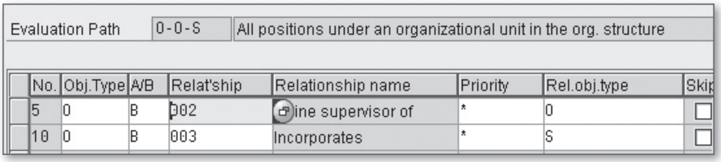
Basically, the structural authorization uses the means of the evaluation paths . Based on a root object, which is defined by its eight-digit object ID, the evaluation path determines all objects under the root object in the structure. The authorization is issued for all of these objects.

[+]

Tip

For more information, refer to the SAP PRESS book, *HR Personnel Planning and Development Using SAP.*

Figure 3.1 illustrates the O-O-S evaluation path as an example. This path lets you access all positions located under a hierarchy of organizational units.



Evaluation Path O-O-S All positions under an organizational unit in the org. structure

No.	Obj.Type	A/B	Relat'ship	Relationship name	Priority	Rel.obj.type	Skip
5	O	B	002	ine supervisor of	*	O	☐
10	O	B	003	Incorporates	*	S	☐

Figure 3.1 O-O-S Evaluation Path

Figure 3.2 shows a structure of organizational units (object type O), positions (object type S), and persons (object type P) as an example. The O-O-S evaluation path describes exactly these object types.

If root object 80000815 is linked to the O-O-S evaluation path, all objects illustrated in Figure 3.2 are permitted. If you specify root object 80004711, an authorization is only issued for the white objects.

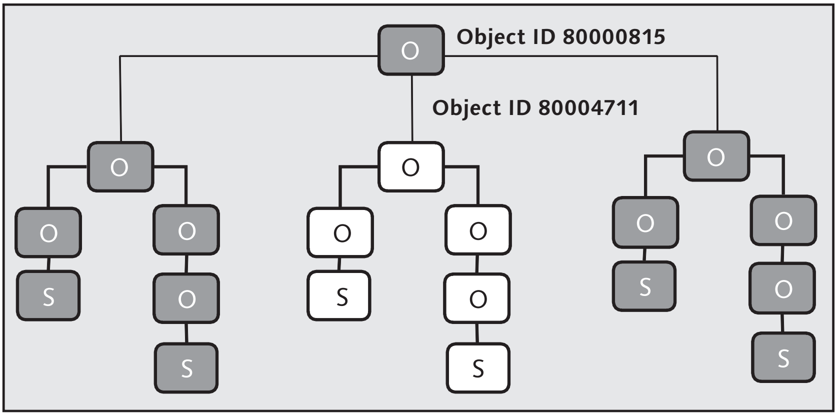


Figure 3.2 Example of a Structural Authorization Check

Flexibility of the structural check

Such an authorization check is completely flexible regarding changes to the structure. For example, if a new organizational unit is — directly or indirectly — assigned to the root object on April 1, 2008, this organizational unit and all linked positions are permitted objects as of April 1, 2008.

[+]

Skipping Object Types

What would you have to do if the authorization was supposed to be issued for the positions but not for the organizational units? And what if you must access the structure via the organizational units because the positions are not hierarchically linked? In this case, you could use the Skip indicator for the evaluation path. If you check the Skip flag in the first row of the O-O-S evaluation path (or in a copy), only the positions (object type S) are permitted, but not the organizational units.

Figure 3.3 provides an overview of the interaction of the general and structural authorization check. Every time objects of the HRP* database table are accessed, the structural and general authorization checks are performed. Only if both checks return a positive result will the authorization be issued.

Now that we've explained the concept of the structural authorization, the following section describes how you can configure structural authorizations.

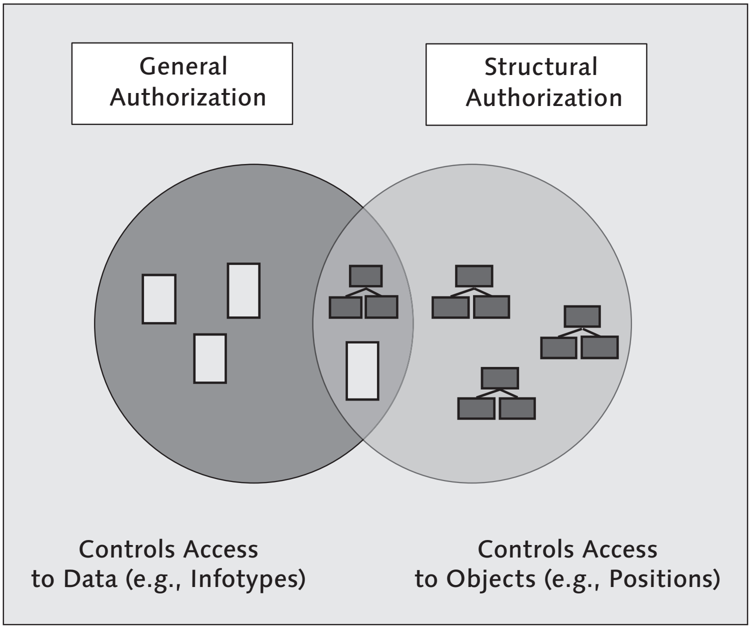

General Authorization
Structural Authorization
Controls Access to Data (e.g., Infotypes)
Controls Access to Objects (e.g., Positions)

Figure 3.3 Interaction of the General and Structural Authorization Checks

3.2 Maintaining the Structural Profiles

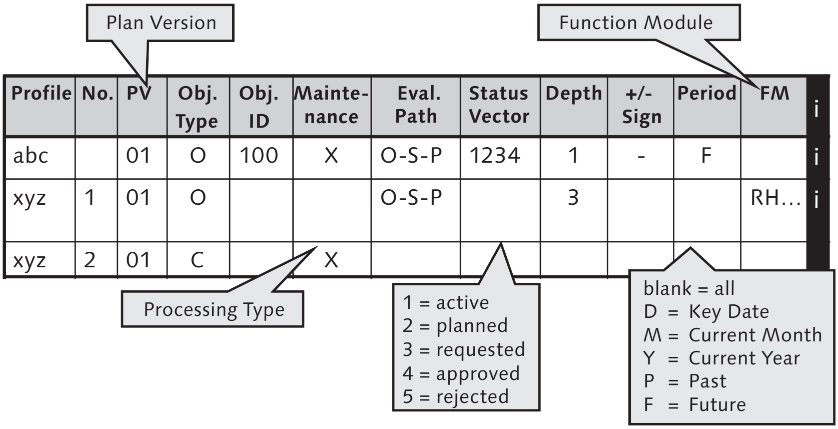
Transaction OOSP

You must maintain the structural profiles outside of the role maintenance (Transaction PFCG) in a specific Transaction called Authorization Profiles (OOSP). Here, the profiles are initially created independently of the users and then, in a second step, assigned to the users (see Section 3.6, Assigning Structural Profiles to Users).

Maintenance parameters in authorization profile maintenance

Figure 3.4 shows the maintenance parameters in the authorization profile maintenance. The fields not shown in the figure are described below:

- **Plan Version|**
  Can be left empty and if so, applies to all plan versions.
- **Object Type**
  (Almost) only internal object types of the HCM system including P (Person) and AP (Applicant). For external objects, structural authorization checks are only performed in exceptional cases (for example, LW – Logistics work center)



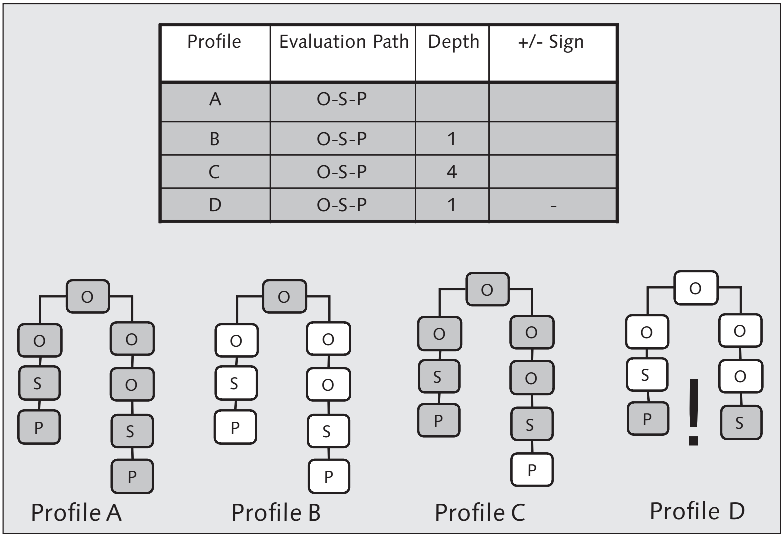
Profile	No.	PV	Obj. Type	Obj. ID	Mainte-nance	Eval. Path	Status Vector	Depth	+/- Sign	Period	FM	i
abc		01	O	100	X	O-S-P	1234	1	-	F		i
xyz	1	01	O			O-S-P		3			RH…	i
xyz	2	01	C		X							

Figure 3.4 Maintenance Parameters in Authorization Profile Maintenance

External Object Types in Structural Authorizations [+]

To determine whether a structural authorization check is performed for an external object, you should use the following path in the IMG: Personnel management • Organizational Management • Basic Settings • Data Model Enhancement• Maintain Object Types • External Object Types. Only if PKEYS is entered in the Key structure field and if the Inverse Relationship flag is checked can you use this external object type in a structural authorization. If you check this, for example, for the cost center, you will determine that you cannot perform a structural authorization check for the cost center in the standard version.

- **Maintenance**
  You can display the object and also maintain its respective infotypes. Table T77FC indicates which functions are supposed to be considered as maintenance functions. The check is only relevant if the maintenance process is also permitted in the general authorization.
- **Depth**
  If the field has the value 0 or is left blank, it indicates that all levels under the root object are permitted; a number refers to the number of the levels permitted under the root object (Figure 3.5).
- **Plus/Minus Sign**
  Reverses the direction for counting the depth (Figure 3.5).



Profile	Evaluation Path	Depth	+/- Sign
A	O-S-P		
B	O-S-P	1	
C	O-S-P	4	
D	O-S-P	1	-

Figure 3.5 Effects of Depth and Plus/Minus Sign

- **Period**
  Here, you define how the responsibility of the structural authorization is checked; for example, whether the user has to be authorized for exactly this key date or only for the year in which he or she accesses the data. See Section 3.7, Period of Responsibility and Time Logic, for more detailed information.
- **Function module**
  The function module is maintained instead of the object ID; for more information, see Section 3.3, Function Modules.

Checking permitted objects

You can find the ℹ button next to the profile description. This button calls the RHAUTH01 report. This report lists the objects that are included in the structural profile and indicates the total number. The button provides an excellent check for whether the structural profile contains all expected object types and object IDs. However, note that the personnel number in the development system or test system has to be assigned to a respective person in Organizational Management if the structural profile determines the permitted objects based on the logged-on user.

The next section describes how a structural profile can dynamically determine the start object instead of entering a defined ID in the Object ID field.

3.3 Function Modules

The structural authorization is pretty flexible. However, entering a defined object ID as a root object is a rigid process and, therefore, requires a lot of maintenance work. Changing the responsibilities in the context of organizational restructuring often affects the structural profiles and particularly the object IDs in this case.

Consequently, when designing the structural authorization, you should always ask yourself whether the number of permitted OM objects can be determined in another way than described previously.

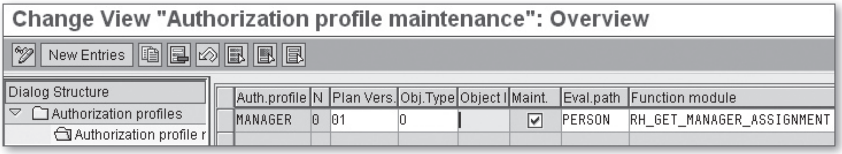
Two examples:

Managers

In this example, a manager who uses the Manager's Desktop or Manager Self-Service is supposed to access the data of the employees he's responsible for.

Usually, the manager's responsibility is already mapped in OM. He holds a position that is linked as a chief position with the subordinate organizational unit. Additional positions and perhaps additional organizational units, including the respective positions, are linked to his organizational unit. The employees for which the manager is responsible hold these positions.

This information enables you to dynamically determine the number of permitted persons, as well as the root object from OM. This is done by the default function module, RH_GET_MANAGER_ASSIGNMENT. In the structural profile, this function module is used instead of the object ID (Figure 3.6).


Change View "Authorization profile maintenance": Overview

Auth.profile	N	Plan Vers.	Obj.Type	Object I	Maint.	Eval.path	Function module
MANAGER	0	01	0		☑	PERSON	RH_GET_MANAGER_ASSIGNMENT

Figure 3.6 Structural Profile with Function Module

Every manager is provided with the same structural profile. The function module determines the root object as follows:

1. It determines the personnel number of the logged-on user via Infotype 0105 (Communication), subtype *SAP User Name* (usually 0001).
2. It reads the position held by the person.
3. It determines the organizational unit with which the position is linked as a manager — this organizational unit is then reported to the structural profile.
4. With the identified object ID, it continues with the stored evaluation path, O-O-S-P in this example, which determines the organizational units, positions, and persons that are linked to the root organizational unit.

Function modules reduce the number of profiles

This tool considerably increases the flexibility of the structural authorization, because it automatically considers all changes that are made under the root object, and the profile can also remain unchanged when the manager changes his position (as long as he is still a manager) or when he or his position is responsible for a different organizational unit. Moreover, you only need one structural profile for all managers.

The second function module supplied by SAP for this purpose is called RH_GET_ORG_ASSIGNMENT. It also determines an organizational unit as a root object, but doesn't use a manager relationship. Instead, the root object is defined by the simple assignment "Position belongs to organizational unit."

Time Administrators

In this second example, time administrators are supposed to be authorized to maintain data of the employees in their own organizational unit.

Customer-specific function modules

If time administrators are also responsible for organizational units to which they are not directly assigned, you must create a specific function module. This is quite simple. First, create a new relationship (e.g., "Is time administrator for") and use it to link the position of the time administrator to another organizational unit. Then, create a new evaluation path by copying the ORGASS default evaluation path and extending it by the customer-specific relationship. Finally, copy the default function module RH_GET_ORG_ASSIGNMENT, and only change the evaluation path in this function module.

Such function modules can use any data from the HCM system or from customer-specific tables to determine the root object.

[+]

Tip

Function modules of this type can return more than one root object. This enables you to determine all authorized objects via the function module, if required, and you don't have to specify an evaluation path at all. The objects can have any object type, which can also deviate from the object type entry in the structural profile.

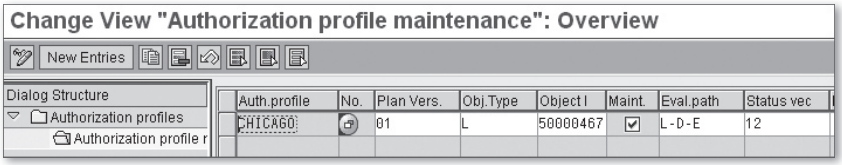
3.4 Transfer to Other Structures in SAP ERP HCM

Structural authorization checks are critical wherever data is stored in HRP* tables. The use of the fields in the profile maintenance fully corresponds to the one described in Section 3.2, Maintaining the Structural Profiles. You can also use the function modules that were introduced in this section.

Components of the HCM system with structural check

The following HCM components outside OM use the structural authorization:

- **Training and Event Management including Learning Solution**
  Here, the business event catalog forms the structure. Figure 3.7 shows a sample restriction of the access to a subcatalog.



Change View "Authorization profile maintenance": Overview

Auth.profile	No.	Plan Vers.	Obj.Type	Object I	Maint.	Eval.path	Status vec
CHICAGO		01	L	50000467	☑	L-D-E	12

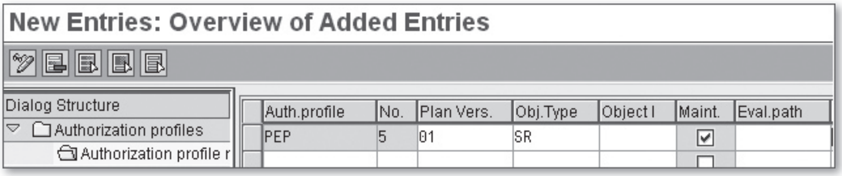
Figure 3.7 Structural Profile with Restriction to Subcatalog

In this case, the root object is a business event group with object ID 50000467; the object types are L (Business event group), D (Business event type), and E (Course).

- **Qualifications**
  It also includes a catalog that defines the structure: the qualification catalog with object types QK (Qualification group), Q (Qualification), and QB (Qualification block), if required.
- **Budget Planning and Position Control (Public Sector)**
  Object type BU (Budget Structure Element) has a hierarchical structure and can be structurally authorized via an evaluation path.

The HCM components mentioned so far each have their own hierarchical structure. The authorizations for these structures use the evaluation path or function module. In addition, there are applications in SAP ERP HCM that don't have a specific structure, but nevertheless entries — without an evaluation path — have to be made in the structural profiles (Figure 3.8). These are all subcomponents, which we haven't mentioned yet, for which the PLOG authorization object is responsible, namely:

- Development plans with object type B (Development Plan)
- Shift planning with object type SR (Planned staff requirement) (Figure 3.8)
- Performance management with object type VA (Appraisal template)
- VB (Criteria Group), and VC (Criterion)
- Management of global employees with object type CP (Central person).


New Entries: Overview of Added Entries

Auth.profile	No.	Plan Vers.	Obj.Type	Object I	Maint.	Eval.path
PEP	5	01	SR		☑	
					□	

Figure 3.8 Structural Authorization for Object Type SR (Requirement)

The structural check cannot be deactivated here

In the HCM components described earlier, the structural authorization is a required supplement to the single OM authorization object, Personnel Planning (PLOG, see Section 2.3.5). All data that is checked with this object is also subject to the structural authorization check. You cannot deactivate this check in the standard version.

However, you can deactivate it for personnel administration, because the structural authorization check is only an option here. We'll describe this option in the next section.

3.5 Use in Personnel Administration

Authorization main switch

If the integration between OM and personnel administration is activated, you can also use the structural authorizations for personnel administration (object type P). In this case, however, the ORGPD authorization switch in the AUTSW group of Table T77S0 must have a value between "1" and "4" (Transaction OOAC (HR: Authorization main switch)). That means, by assigning a value other than 0, you activate the structural authorization for personnel administration. Section 3.8, How the Structural Authorization Check Handles Nonintegrated Persons, explains the different meaning of the values "1" through "4."

The structural authorization check in personnel administration also uses the flexibility of the structural authorization already described also for personnel master data and time data. It represents an alternative for using:

- The Organizational Key field in the P_ORGIN (HR: Master Data) authorization object.
- The different administrator IDs of Infotype 0001 in the P_ORGXX (HR: Master Data – Extended Check) authorization object.

As long as the organizational assignment of the persons is reliably maintained in OM, you don't have to maintain the mentioned fields in Infotype 0001 if you use the structural authorization.

[Ex]

Example

Managers are only authorized to view a specific selection of infotypes for the employees of their organizational units.

For this purpose, the structural profile, MANAGER, described in Section 3.3, Function Modules, is required. In the HR: Master Data object, you only have to list the infotypes under INFTY and the R authorization level. No organizational restrictions are required.

You must consider the following aspects for maintaining the structural profiles in conjunction with the infotypes of personnel administration:

- The evaluation path in the profile maintenance must include object type P.
- The combination of the structural authorization with the organizational fields of the authorization objects, *HR: Master Data a*nd *HR: Master Data – Extended Check,* is an AND link. That means the check of the default object and the structural check both have to be successful to assign an authorization.

Disadvantages of the structural authorization check

Although the structural authorization is the preferred method for personnel administration in most cases, you must take the following into account: The fully accurate maintenance of Organizational Management is an essential prerequisite for a consistent structural authorization protection; however, the structural authorization is more complex than the general authorization alone. Consequently, there's a great deal of learning effort involved for the affected administrators, as well as testing effort for configuring and changing the authorizations.

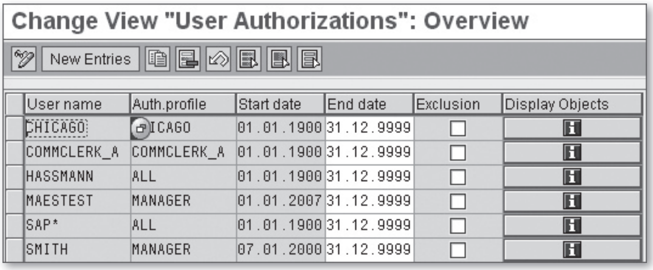
[+]

Tip

You can also activate the structural authorization check in the (classic) recruitment using a switch. See Chapter 5 for more detailed information.

3.6 Assigning Structural Profiles to Users

Transaction OOSB (User Authorizations), shown in Figure 3.9, is used to assign the profiles to users.



Change View "User Authorizations": Overview

User name	Auth.profile	Start date	End date	Exclusion	Display Objects
CHICAGO	ICAGO	01.01.1900	31.12.9999	☐	i
COMMCLERK_A	COMMCLERK_A	01.01.1900	31.12.9999	☐	i
HASSMANN	ALL	01.01.1900	31.12.9999	☐	i
MAESTEST	MANAGER	01.01.2007	31.12.9999	☐	i
SAP*	ALL	01.01.1900	31.12.9999	☐	i
SMITH	MANAGER	07.01.2000	31.12.9999	☐	i

Figure 3.9 Assigning Profiles to Users

In this transaction, the structural profiles — together with a validity period — are assigned to the users. A user may have several structural profiles.

If you check the Exclusion field, the profile is negative, that is, it indicates all objects that the user is not authorized to view or edit. The Information button works in the same way as in profile maintenance: It displays the permitted objects.

Fall-back to SAP*

What happens if the table doesn't contain entries for a specific user? In that case, the authorization check uses the entry of the SAP* user. So, the profile stored for this user is applicable if an entry has been left out. That means you have two possible alternatives:

Alternative 1

Leave everything as it has been provided by SAP: SAP* provides an ALL profile that contains the full structural authorization for all object types. This is advisable if you use the structural authorization only for a small user community, and if the other users were assigned with an unrestricted structural authorization anyway.

Alternative 2

If you want to avoid a user that isn't assigned to a profile at all, that is, if you don't want a structural authorization to be issued in this case, you must create an "empty profile" and assign it to the SAP* user. The "empty profile" could, for example, contain only an object type that you don't use. Alternatively, you can delete the entry for SAP*. In this case, too, the user to which no structural profile is assigned doesn't have an authorization.

These two variants are useful if you have to maintain multiple structural authorizations. They prevent you from assigning the SAP* authorization to users by mistake that aren't supposed to have this authorization.

[!]

This becomes more important if Transaction OOSB (User Authorizations) does NOT check the user's input.

[+]

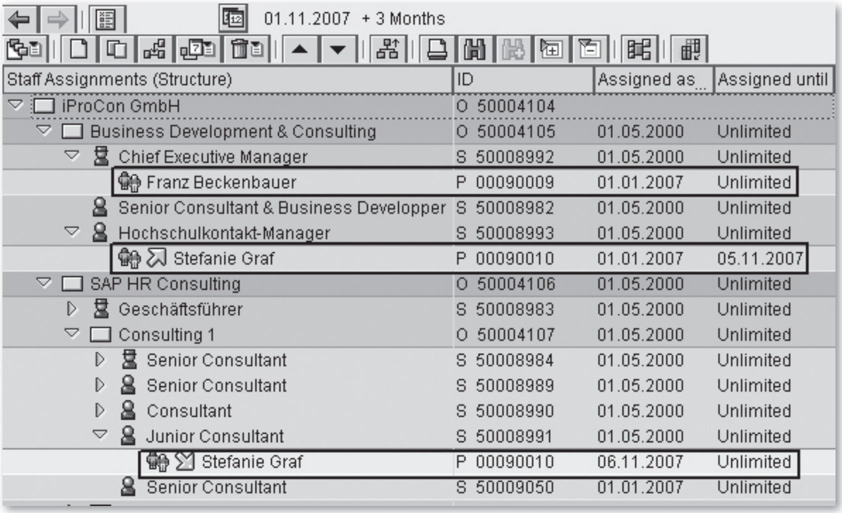
Assigning a Profile to the SAP* User

If most of the users are supposed to get the same profile, it may be useful to assign this profile to the SAP* user.

Let's look at an example: All time administrators are authorized to edit data of the employees in their own organizational unit. If an enterprise had 10,000 employees, approximately 100 time administrators would have the same structural profile with the RH_GET_ORG_ASSIGNMENT function module. If you assign the time profile — instead of the 100 entries — to the SAP* user, you can avoid a great deal of maintenance effort. At the same time, it would be a minimum fall-back profile for users who haven't been assigned by mistake.

3.7 Period of Responsibility and Time Logic

In Organizational Management, all relationships have a *validity period*. For example, if an employee changes the organizational unit and is transferred to a new position, a new relationship period for the new position starts (Figure 3.10).

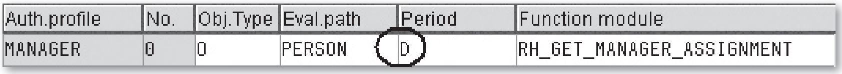


01.11.2007 + 3 Months

Staff Assignments (Structure)	ID	Assigned as...	Assigned until
iProCon GmbH	O 50004104		
Business Development & Consulting	O 50004105	01.05.2000	Unlimited
Chief Executive Manager	S 50008992	01.05.2000	Unlimited
Franz Beckenbauer	P 00090009	01.01.2007	Unlimited
Senior Consultant & Business Developper	S 50008982	01.05.2000	Unlimited
Hochschulkontakt-Manager	S 50008993	01.05.2000	Unlimited
Stefanie Graf	P 00090010	01.01.2007	05.11.2007
SAP HR Consulting	O 50004106	01.05.2000	Unlimited
Geschäftsführer	S 50008983	01.05.2000	Unlimited
Consulting 1	O 50004107	01.05.2000	Unlimited
Senior Consultant	S 50008984	01.05.2000	Unlimited
Senior Consultant	S 50008989	01.05.2000	Unlimited
Consultant	S 50008990	01.05.2000	Unlimited
Junior Consultant	S 50008991	01.05.2000	Unlimited
Stefanie Graf	P 00090010	06.11.2007	Unlimited
Senior Consultant	S 50009050	01.01.2007	Unlimited

Figure 3.10 Stefanie Graf Changes the Organizational Unit as of 11/06/2007

When maintaining the structural profiles (Transaction OOSP), you can restrict the structure's validity period to the current key date (Figure 3.11), current month, current year, past, or future (see Section 3.2, Maintenance of the Structural Profiles).



Auth.profile	No.	Obj.Type	Eval.path	Period	Function module
MANAGER	0	0	PERSON	D	RH_GET_MANAGER_ASSIGNMENT

Figure 3.11 The Analysis of All Persons the Manager is Responsible for is Carried out on the Key Date (D)

Therefore, for this restriction it is always checked whether there is an intersection with the relationship period along the structure. If the check can be carried out down to the lowest level — the person — the period of responsibility is identical with the relationship period (between person and position).

In the following section, the different values are described that the periods of responsibility for the leads of Org Units A1 and A2 can have in the PERIOD column. You can also use Figure 3.12 for orientation. A structural profile as shown in Figure 3.11 and the system date 11/06/2007 are required:

- **Period = D (Key Date)**
  Only the manager of OrgUnit A2 can view the person (11/06/2007).
- **Period = F (Future)**
  Only the manager of OrgUnit A2 can view the person (11/06/2007 to 12/31/9999).
- **Period = M (Month)**
  Both leaders can view the person (11/01/2007 to 11/30/2007).
- **Period = Y (Year)**
  Both leaders can view the person (01/01/2007 to 12/31/2007).
- **Period = P (Past)**
  Only the manager of OrgUnit A1 can view the person (01/01/1800 to 11/05/2007).

- **Period = Blank (All)**
  Both leaders can view the person (01/01/1800 to 12/31/9999).

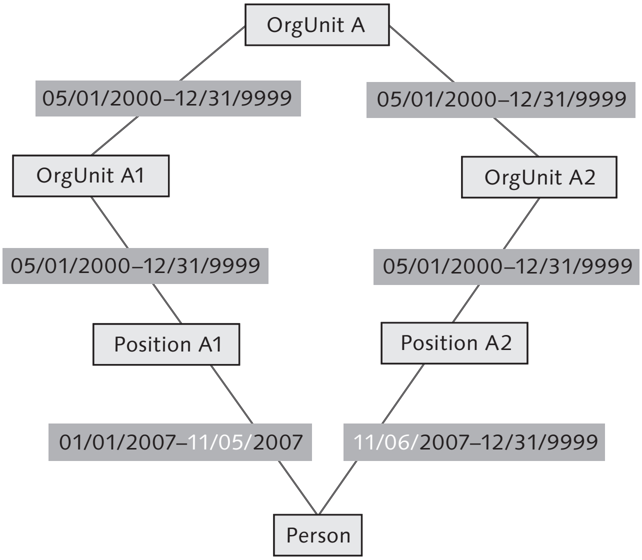
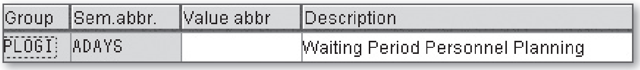


Figure 3.12 Organizational Change as of 11/06/2007 – Diagram

Grace period for structure period

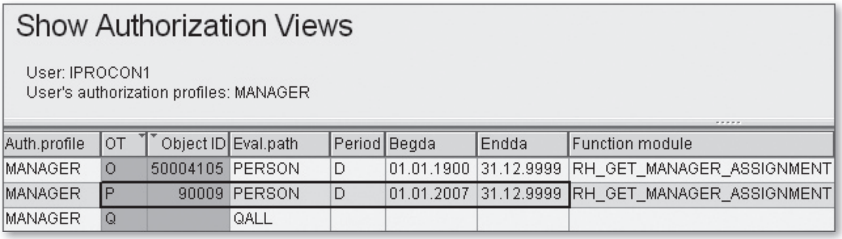
The PLOGI ADAYS authorization switch extends the validity period of the structural profile. By default, the default value of the switch is blank (Figure 3.13).



Group	Sem.abbr.	Value abbr	Description
PLOGI	ADAYS		Waiting Period Personnel Planning

Figure 3.13 Standard Version of PLOGI ADAYS

This setting in combination with the key date validity of the analysis of the persons (see Figure 3.11) would mean that the leader, Franz Beckenbauer (see Figure 3.10), can no longer view his employee, Stefanie Graf, as of 11/06/2007. You can quickly check this by selecting the ℹ button in the assignment of the profile to the user (Transaction OOSB) or starting the RHAUTH01 (Show Authorization Views) report. The result is shown in Figure 3.14.



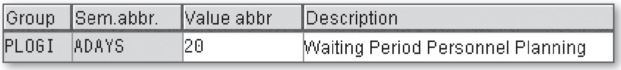
Show Authorization Views

User: IPROCON1
User's authorization profiles: MANAGER

Auth.profile	OT	Object ID	Eval.path	Period	Begda	Endda	Function module
MANAGER	O	50004105	PERSON	D	01.01.1900	31.12.9999	RH_GET_MANAGER_ASSIGNMENT
MANAGER	P	90009	PERSON	D	01.01.2007	31.12.9999	RH_GET_MANAGER_ASSIGNMENT
MANAGER	Q		QALL				

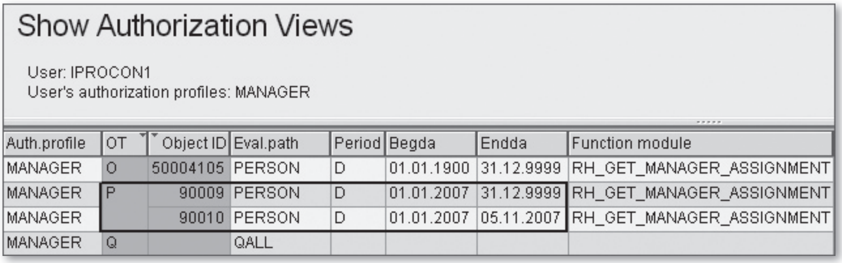
Figure 3.14 The Manager Can No Longer View His Employee as of 11/06/2007

Set the grace period above the PLOGI ADAYS authorization switch to 20 days (Figure 3.15), for example. Then, Franz Beckenbauer can view his employee again (Figure 3.16).



Group	Sem.abbr.	Value abbr	Description
PLOGI	ADAYS	20	Waiting Period Personnel Planning

Figure 3.15 Grace Period of 20 Days



Show Authorization Views

User: IPROCON1
User's authorization profiles: MANAGER

Auth.profile	OT	Object ID	Eval.path	Period	Begda	Endda	Function module
MANAGER	O	50004105	PERSON	D	01.01.1900	31.12.9999	RH_GET_MANAGER_ASSIGNMENT
MANAGER	P	90009	PERSON	D	01.01.2007	31.12.9999	RH_GET_MANAGER_ASSIGNMENT
MANAGER		90010	PERSON	D	01.01.2007	05.11.2007	RH_GET_MANAGER_ASSIGNMENT
MANAGER	Q		QALL				

Figure 3.16 Extension of the Relationship Using PLOGI ADAYS

[!]

Maintaining PLOGI ADAYS

You won't find the PLOGI ADAYS authorization switch in the Maintain Authorization Main Switches IMG activity, where the other switches of the AUTSW group can be found. To maintain the PLOGI ADAYS switch, navigate directly to the table maintenance of T77S0. Don't get confused by the documentation for this switch ((F1) help). It's incorrectly identical to the documentation for the AUTSW ADAYS authorization switch (see Section 2.6, Period of Responsibility and Time Logic). SAP Note 375216 explains the functionality of this switch, which is available from Release 6.20 onward, in more detail.

AUTSW ADAYS and PLOGI ADAYS combined

If you use the general and structural authorization with both authorization switches, the following applies for our example of an organizational change as of 11/06/2007, as well as the key date 11/06/2007:

1. As long as the manager, Franz Beckenbauer, cannot view his employee, Stefanie Graf, via the structural profile, he cannot do anything.
2. If you extend the structural profile by a grace period using PLOGI ADAYS, the manager can view Stefanie Graf and read/analyze her data for the past. However, he cannot maintain infotypes (for which the access authorization in Table T582A is activated) for Stefanie Graf.
3. If the period of responsibility of the general authorization is additionally extended via AUTSW ADAYS, the manager can maintain infotypes for Stefanie Graf for this tolerance period.

Best practice

Usually, a blank in the date field is sufficient for the structural profiles of central areas. For decentralized profiles, use Y for users with read access and D for users with write access for further restrictions.

Summary

Let's summarize the essential aspects for the periods of responsibility and time logic once again:

- The period check of the structural authorization is executed prior to the period check of the general authorization.
- The period of responsibility of the structural authorization arises from the last relationship period if the check has a positive result.
- The period of responsibility is transferred to the general authorization and further restricted, if required.
- The period check can be extended by a tolerance period — in the general authorization using the AUTSW ADAYS authorization switch and in the structural authorization using the PLOGI ADAYS authorization switch.

Of course, the responsibility period and period checks can only be performed for persons that are linked to the organizational structure. However, specific person groups (for example, trainees or retirees) are often not included in the organizational structure. The next section describes how the system handles nonintegrated persons.

3.8 How the Structural Authorization Check Handles Nonintegrated Persons

In personnel administration, the structural authorization only records persons that are integrated in Organizational Management. Persons that are excluded from the integration via the PLOGI characteristic are not considered in the structural check. This also applies to persons for which no position has been entered in Infotype 0001, that is, the infotype still contains the default position (usually 99999999).

Linking the nonintegrated persons with the organizational structure via special evaluation paths such as the temporary assignment relationship doesn't solve the problem. The structural check still ignores nonintegrated persons.

Authorization main switch

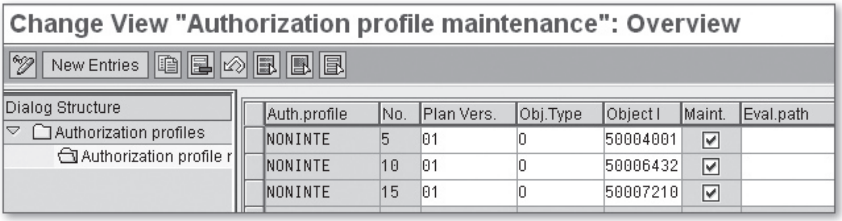
To control how these persons are handled with regard to authorizations, the authorization switches, AUTSW ORGPD and AUTSW DFCON, are provided. Their values 1 to 4 have the same meanings. ORGPD controls the normal authorization check while DFCON controls the context-sensitive check. You can maintain the switches via IMG path PERSONNEL MANAGEMENT • PERSONNEL ADMINISTRATION • TOOLS • AUTHORIZATION MANAGEMENT • MAINTAIN AUTHORIZATION MAIN SWITCHES • MAINTAIN AUTHORIZATION MAIN SWITCHES.

Rules for checking nonintegrated persons

Initially, the four switch settings enable you to use the ORGANIZATIONAL UNIT field of Infotype 0001 for the authorization check. If you want to use the settings, you must enter all authorized organizational units separately into the structural profile (see example in Figure 3.17). Then, you must decide whether the authorization is supposed to be rejected or issued if an organizational unit is missing. This results in the following combinations:

- Switch setting 1: The organizational unit is analyzed, no authorization is issued if it is not maintained.
- Switch setting 2: The organizational unit is not analyzed, an authorization for persons without an integrated position is generally rejected (makes only sense if all persons are integrated).

- Switch setting 3: The organizational unit is analyzed, an authorization is issued if it is not maintained.
- Switch setting 4: The organizational unit is not analyzed, an authorization for persons without an integrated position is generally issued.


Change View "Authorization profile maintenance": Overview

Auth.profile	No.	Plan Vers.	Obj.Type	Object I	Maint.	Eval.path
NONINTE	5	01	O	50004001	☑	
NONINTE	10	01	O	50006432	☑	
NONINTE	15	01	O	50007210	☑	

Figure 3.17 Organizational Units for Nonintegrated Persons

[+]

Exceptions for DFCON

While switch setting 0 of the ORGPD switch deactivates the structural authorization check for personnel master data, the DFCON authorization switch differentiates between 0 and 1 as follows (see SAP Note 647278):

1: Only users with unrestricted access (that is, "*" in all fields of the context-dependent authorization object including the PROFL field) can access nonintegrated persons whose organizational unit is not maintained.

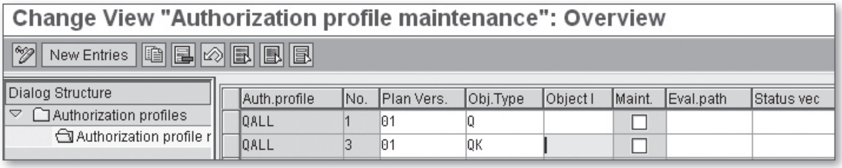
0: Users with restricted master data access (for example, for personnel areas) but "*" in the PROFL field can also access nonintegrated persons whose organizational unit is not maintained.

3.9 Performance Optimization

The performance of the structural authorization check results from the number of read accesses required to determine whether a specific object is permitted or not. The larger the number of different object types with different evaluation paths contained in the profile and the more objects that exist under the root, the longer the access times.

Use as few evaluation paths as possible

If some object types may be viewed completely, such as the entire qualification catalog, the evaluation path shouldn't contain a root object and evaluation path (Figure 3.18).

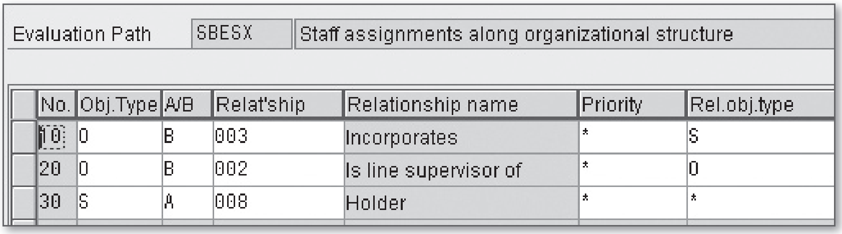

Change View "Authorization profile maintenance": Overview

Auth.profile	No.	Plan Vers.	Obj.Type	Object I	Maint.	Eval.path	Status vec
QALL	1	01	Q		☐		
QALL	3	01	QK		☐		

Figure 3.18 Profile Without Evaluation Path

An additional potential for optimization is to use as few evaluation paths as possible. For example, combine all object types that you determine via the organizational structure into one evaluation path. Have the structural check read the organizational hierarchy only once in order to determine all permitted organizational units, positions, persons, jobs if required, work centers, and so on.

In addition, make sure that only evaluation paths with a specified target object are used. The evaluation path illustrated in Figure 3.19, lists all objects linked to the position. Depending on the system landscape, this may include, for example, object types US (User) or BP (Business Partner), which then would be unnecessarily included in the structural check.


Evaluation Path SBESX Staff assignments along organizational structure

No.	Obj.Type	A/B	Relat'ship	Relationship name	Priority	Rel.obj.type
10	O	B	003	Incorporates	*	S
20	O	B	002	Is line supervisor of	*	O
30	S	A	008	Holder	*	*

Figure 3.19 Evaluation Path With Nonspecified Target Object

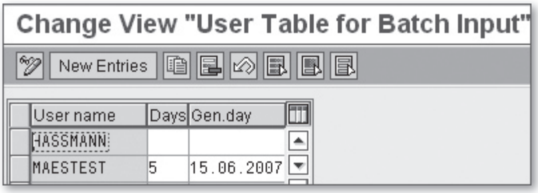
Buffering large data quantities

The optimization measures described so far reach their limits when users are authorized to view or edit a large quantity of objects of the structural check. In this case, the structural check, which is carried out online on an ongoing basis, leads to unacceptable response times. For these situations, a procedure is provided by default. It enables you to store the information on the permitted objects of a user in the SAP memory. Then, the accesses to the SAP memory have a high performance.

As a prerequisite, you must enter the affected users (it doesn't have to and shouldn't include all users) in Table T77UU. There are two possible alternatives:

Manual maintenance in the IMG

You can maintain Table T77UU manually in IMG activity Personnel Management • Organizational Management • Basic Settings • Authorization Management • Structural Authorization • Save User Data in SAP Memory. Here, you enter the number of days that are supposed to pass between the automatic updates of the SAP memory for the respective user. The date of the last update of the system is stored here as well (Figure 3.20).



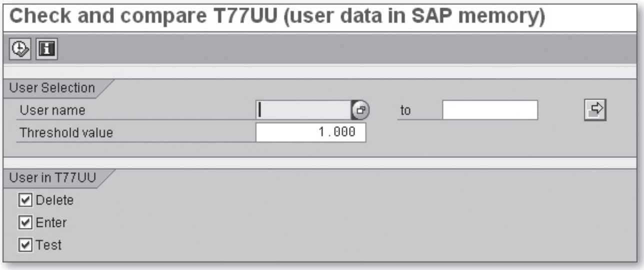
Change View "User Table for Batch Input"

User name	Days	Gen.day
HASSMANN		
MAESTEST	5	15.06.2007

Figure 3.20 Maintaining Table T77UU – User with SAP Memory

Automatic maintenance using RHBAUS02

Instead of maintaining Table T77UU manually, you can also use the RHBAUS02 report (Check and Compare T77UU (User Data in SAP Memory)). In the standard system, you can start the report only via System • Services • Reporting (Transaction SA38). The report maintains Table T77UU by means of a threshold value. The value results from the number of permitted objects that correspond to the structural authorization. When the report is executed (as shown in Figure 3.21), the system enters all users with an object quantity above 1,000 in Table T77UU or deletes users with an object quantity below this value from the table.



Check and compare T77UU (user data in SAP memory)

User Selection

User name ____ to ____

Threshold value 1.000

User in T77UU

☑ Delete

☑ Enter

☑ Test

Figure 3.21 RHBAUS02 Report – Check and Compare T77UU

Regardless of your entries in Table T77UU, if the Days field is left empty, the SAP memory is not automatically supplied. Instead, you must ensure that the RHBAUS00 (Regeneration INDX for Structural Authorization) report runs properly. You can start it in batch mode on a regular basis (for example, hourly), or it can run online, if required. It runs for the users that have been defined in the selection screen.

The consequence of all procedures of regular SAP memory updates described previously is that changes to the objects, for example, the organizational structure, for the defined users reach the authorizations with a delay.

[+]

Tip

The online update of the SAP memory is not supported in the standard version. SAP Note 421399 provides information on how you can modify the standard settings.

There are situations in which even the SAP memory reaches its performance limits. This is the case when the SAP memory area provided for authorization purposes gets too small due to a considerably large number of users with a high quantity of permitted objects. In these cases, the structural authorization check must be replaced by a customer-specific authorization check for this user category. For this purpose, you can use the Business Add-In (BadI) of the structural authorization check, HRBAS00_STRUAUTH. This BAdI is described in greater detail in the following section.

3.10 Extensions

BAdIs enable you to implement requirements for the authorization check that exceed the SAP standard without having to modify it. They also enable you to change the standard coding at places predefined by SAP and implement customer-specific checks. From Release 4.6C onward, the authorization check provides a BAdI for the structural authorization check.

If nothing else helps

The HRBAS00_STRUAUTH BAdI is called for any structural authorization check before the check is actually executed. Then, the BAdI allows you to issue or reject the structural authorization while avoiding the standard checks.

You can find the BAdI in the IMG via Personnel Management • Organizational Management • Basic Settings • Authorization Management • Structural Authorization • BAdI: Structural Authorization. The corresponding documentation is also provided here.

The BAdI is comprised of six methods; two of them are described below as examples:

- **CHECK_AUTHORITY_VIEW**
  This method serves to check the structural authorization of a user for an object. This method is supposed to reduce runtime problems. As a result of the check in this method, you obtain the information that the user has or doesn't have authorization for a specific object or that a new object to be checked (CHECK_OBJECT_OUT) is transferred. In that case, the standard check with the built-up view is used. You can control this by setting the transferred EXIT_FLAG switch to initial. If you don't want to use the standard coding, you must set the switch to "X."
- **CHECK_AUTHORITY_SEARCH**
  This method serves to check the structural authorization within the Search Function or the input help. For this purpose, the hit list is transferred for clean-up purposes. The plan version that is supposed to be checked and the permitted object types are transferred to the method in the PLVAR and OTYPES parameters. In addition, the complete hit list is available in the OBJECTS table that can be changed if required. The check deletes all entries from the hit list for which the user doesn't have a structural authorization.
  If you set the SKIP_STANDARD switch to "X" upon return, the search function doesn't execute another structural authorization. If you set the SKIP_STANDARD switch to " " (blank), the standard check of the structural authorization is performed.

Examples

At this point, we want to provide some examples of how you can use BAdIs.

Insufficient SAP memory

For users with central authorizations in Organizational Management, the response times were insufficient although the SAP memory was used. This was probably caused by the large number of this category of users.

Consequently, for a specific user community within the BAdIs, the structural authorization check was deactivated and replaced by a customer-specific authorization check. In the maintenance of the structural profiles, the respective users were identified by a specific profile. Because this profile issues unrestricted structural authorizations, it doesn't fill the table of the permitted objects.

The BAdI recognizes that the structural check hasn't been performed by the name of the profile and navigates to the check of a customer-specific authorization object. This object contains the company codes for which the user is authorized. The BAdI checks whether the object of Organizational Management that is supposed to be checked is linked with a permitted company code.

The company code is a standard object type of OM called IC. The relationship to the company code is written with a customer-specific program, which is continuously running.

Training and Event Management

To enable administrators or assistants to book a business event for an employee, they require a maintenance authorization for the event. However, if the business event catalog is exclusively maintained centrally, a conflict in the authorization assignment arises. The HRBAS00_STRUAUTH BAdI must be used in order to allow for access to specific person groups regardless of the action to be performed (for example, booking an event for all employees, analyses and follow-up processing only for a selection of employees). In general, the structural authorization is granted if all actions are allowed for a group of employees. In other cases, the BAdI controls the access to employees depending on the transaction. It may cause problems that different actions in SAP Training and Event Management are sometimes executed with identical transactions. As an alternative, you can define in the BAdI that the structural authorization is only supposed to be assigned to employees with restricted actions, and that the access authorization for these employees is withdrawn for other transactions.

Missing Organizational Management

Assistants are supposed to maintain business trips for selected persons. However, they don't use Organizational Management. That means, it is no longer possible to check any authorization via the organizational structure. The permitted personnel numbers are assigned to the assistant in a Customizing table. This table is queried by BAdI HRBAS00_STRUAUTH.

[+]

Tip

For BAdI HRBAS00_STRUAUTH, you must always implement all methods. Immediately after creating the implementation, you can find a sample coding in the menu via Goto • Sample Code • Display or in the CL_EXM_IM_HRBAS00_STRUAUTH class.

3.11 Critical Success Factors

The following section describes some critical success factors that you must take into account when using the structural authorization check:

- Keep your Organizational Management reliably maintained and up-to-date. Maintenance is reliable only if Organizational Management is integrated with personnel administration. As soon as the structural authorization is used, the maintenance in Organizational Management can directly affect the authorizations.
- In the structural authorization check, you should use as many function modules as possible and simplify the maintenance in this way. For this purpose, it is always useful to use the existing information of Organizational Management via function modules.
- Pay attention to the response times, particularly for users that can access multiple objects. If required, use the optimization options described in Section 3.9, Performance Optimization. As your Organizational Management usually grows along with the increasing number of components you implement and the longer it is in use, you should check the performance for critical users carefully at regular intervals.
- Cautiously determine which of the variants of handling SAP* described in Section 3.6, Assigning Structural Profiles to the Users, you want to select. In any case, make sure that not too many authorizations are assigned by mistake.
- Don't forget to implement appropriate authorization protection for people not integrated with Organizational Management (see Section 3.8, How the Structural Authorization Check Handles Nonintegrated Persons).

Index