Context-Sensitive Realization of the Authorization Check in HR Master Data

Nada Moalla
Christiane von Rekowski
07.12.2001

Contents

1 Authorizations in *mySAP HR*

Authorizations control system users' access to system data and are therefore a fundamental prerequisite for the implementation of business software. In Human Resources, authorizations play a significant role since access to personal data must be strictly controlled.
There are two main ways to set up authorizations for *mySAP Human Resources*:

- You can set up *general authorizations* that are based on the SAP-wide authorization concept
- You can set up HR-specific *structural authorizations*

1.1 General Authorization Check in *mySAP HR*

The general Authorization Check for *mySAP HR* controls access to *Human Resources* infotypes and forms part of the general SAP authorization check.
Authorizations from general authorization checks are described by Authorization Objects. An authorization object defines the fields that occur in an authorization. The system checks if a user has the corresponding authorization in the user master record for certain field specifications. Authorizations are grouped together in Authorization Profiles. A user's authorizations are determined from the authorization profiles assigned to the user in the master data record for the different authorization objects in the system.

Example:

The authorization object P_ORGIN is used during the authorization check on HR infotypes. This check takes place when HR infotypes are edited or read.
P_ORGIN contains the following fields, which are tested during an authorization check:

Authorization Field	**Long Text**
INFTY	Infotype
SUBTY	Subtype
AUTHC	Authorization Level
PERSA	Personnel Area
PERSG	Employee Group
PERSK	Employee Subgroup
VDSK1	Organizational Key

The AUTHC field (Authorization Level) also contains the access mode for the authorization (for example, **R** = Read).

You can create and edit authorization objects using the transaction SU21. You can use Role Maintenance (transaction PFCG) to create authorization profiles and to assign users.

The use of authorization objects in the area of HR Master Data is controlled mainly by Authorization Main Switches.

1.2 Structural Authorization Check in *mySAP HR*

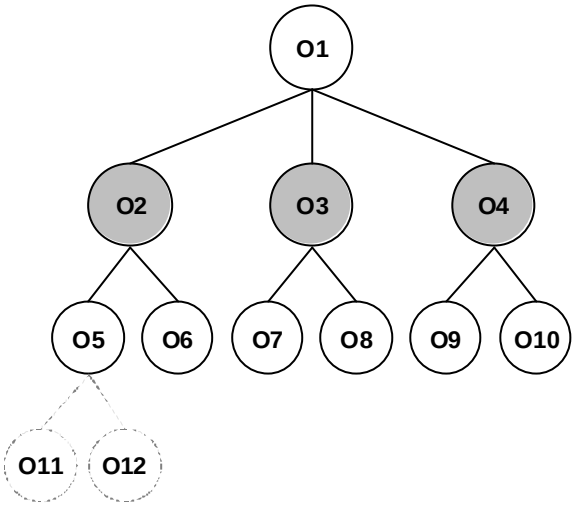
On top of the general authorization check, which is based on authorization objects, you can define additional authorizations by hierarchical structures (for example, organizational structures) called *structural authorizations*.
You can use the structural authorization check to define authorizations in the following areas:

- Plan versions
- Object types

- Object IDs

In each area, the combination of start object and Evaluation Path from an existing structure returns a specific number of objects. This exact combination, in other words the number of objects returned by this combination, represents a user's structural profile. The structural authorization check is therefore based on a dynamic concept: The concrete objects that are returned by a structural profile change as the structure (under the start object) changes.

Example:

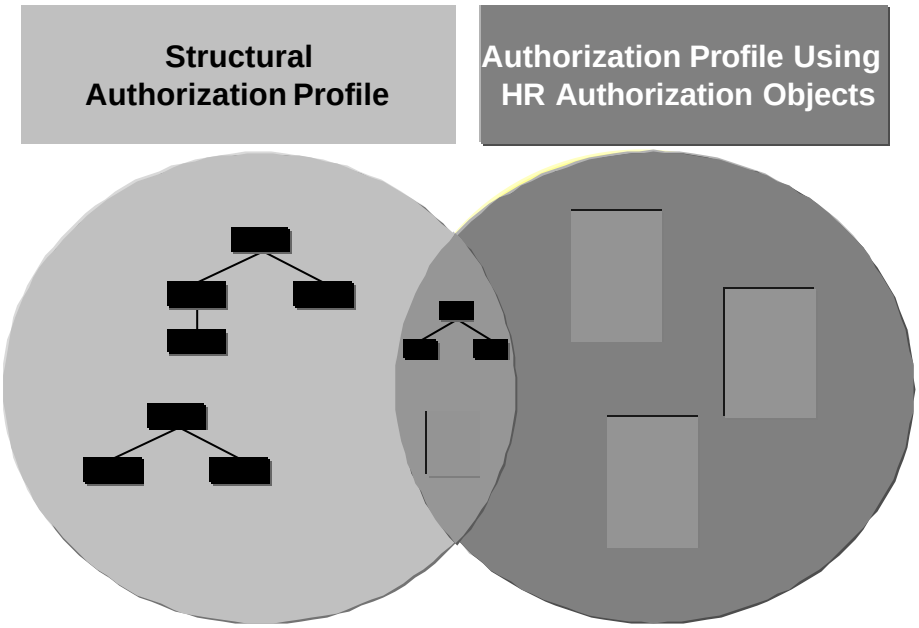


The organizational structure is expanded to include the organizational units O11 and O12. Because you are using the structural authorization check, you do not have to expand profiles such as *O2 and lower-level objects* additionally.

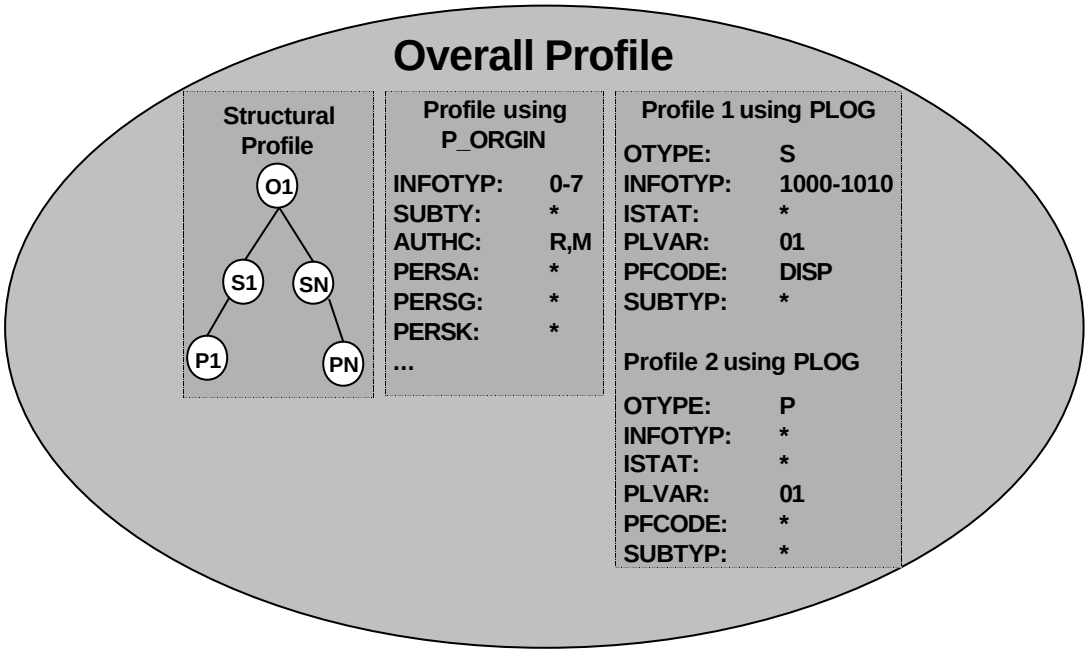
Structural profiles are assigned in a different way to general authorization profiles. To assign structural profiles, you use table T77UA (*User Authorizations = Assignment of Profile to User*), not Role Maintenance (PFCG transaction) as with general authorization profiles. The authorization profiles are specified in the T77PR table (*Definition of Authorization Profiles*). You can protect (sub)structures by making relevant entries in this table.

1.3 Overall Profiles

A user's Overall Profile is determined from the intersection of his or her structural and general authorization profiles, when you use both structural and general authorizations.
The structural profile determines which object in the hierarchical structure the user has access to; the general profile which object data (infotype, subtype) and which type of authorization (Read, Write, ...) the user has for these objects. The access mode for authorization objects in HR Master Data is determined in the AUTHC field (Authorization Level).



An overall profile could be put together as follows, for example:

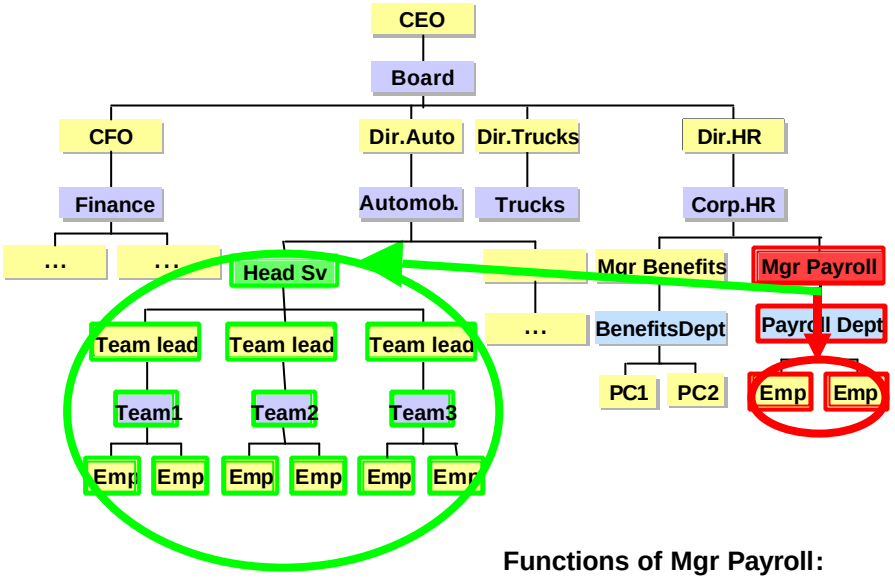


The following authorizations or restrictions are valid for a user who has the overall profile illustrated above:

- The user has a read authorization for the positions S1 to SN in the infotypes 1000 to 1010 (structural profile and 1/PLOG profile).
- The user is not authorized to access organizational units with this profile since the user has no corresponding PLOG authorization.
- The user has a read authorization for the persons P1 to PN in the infotypes 0 to 7 (structural profile and profile/P_ORGIN).
- Note: For the user to be able to access data on persons, you need to assign the user a corresponding PLOG authorization for persons. However, the infotype must be unspecified (profile 2/PLOG).

2 Context Problems in HR Authorizations

The technical separation of general and structural authorization profiles can cause context problems for users who perform different Roles in a company (see graphic). This is due to the fact that you cannot simply add any number of structural and general authorization profiles required for different tasks (in different contexts) without overriding something.



Example:

A user (referred to as manager 1 in this example) is the *manager* of a team and should be allowed to edit infotypes 0000 – 0007 for the employees in his or her team.
Manager 1 is also *Payroll Manager* for another organizational structure. In this second role, manager 1 has access to all payroll-relevant infotypes (0008 and 0015) for the employees in this organizational structure.

The business requirements of the roles *Manager* and *Payroll Manager* are represented again in the following overview table:

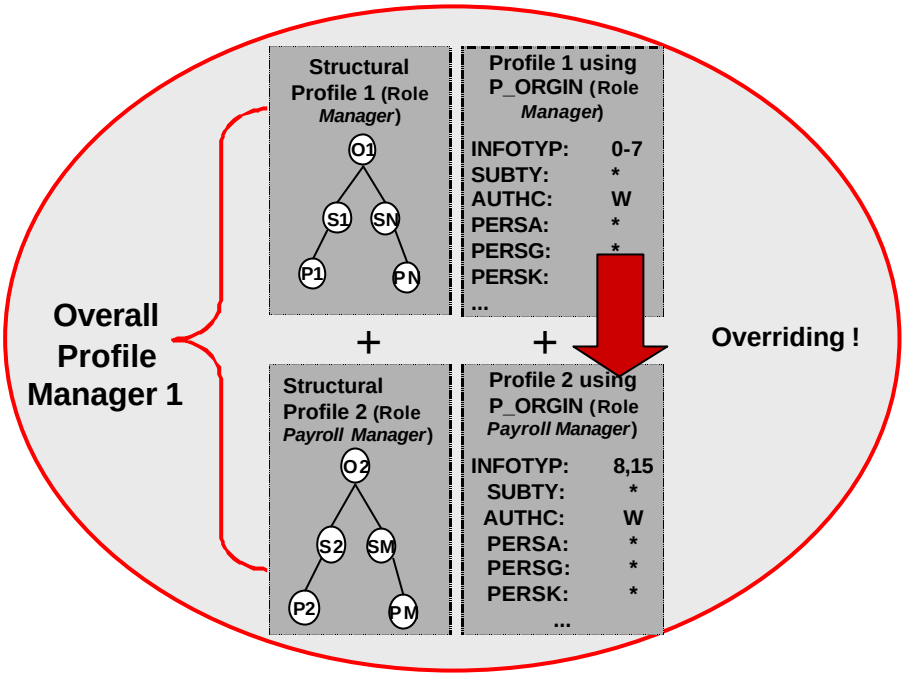
Business overall profile of the role *Manager*:

Objects	Type of Authorization
All employees in the manager's team	Full read and write authorization for infotypes 0000 to 0007

Business overall profile of the role *Payroll Manager*:

Objects	Type of Authorization
Employees in the organizational structure	Full read and write authorization for infotypes 0008 to 0015

This cannot be illustrated using the existing HR authorization concept because there is no relationship of any kind between an individual structural profile and an individual basis authorization. This leads to something being overridden.



You cannot create an assignment between a specific structural profile of a user (here, for example, structural profile 2) and a specific general profile (profile with P_ORGIN).
What in fact happens is that the system adds the structural profiles (that is the set of objects) and the general profiles (in this case, using P_ORGIN) to the overall profile. Consequently, the following effect occurs in the above example: Manager 1 has complete read and write authorization for all objects in both structural profiles. When the authorization profiles are added together, the following overall profile is produced:

Objects	Type of Authorization
All employees in the manager's team and organizational structure	Full read and write authorization for infotypes 0000 to 0008 and for 0015

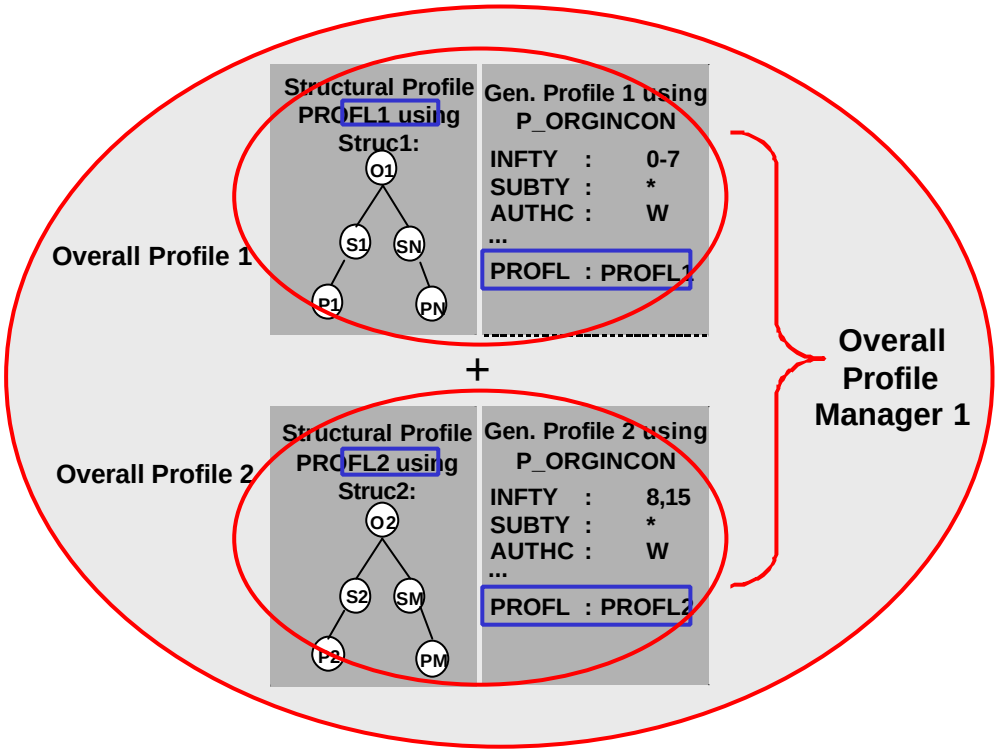
2.1 Workaround

If you use a separate user for each context, it is easier to map different contexts (roles) with the correct authorization.
For example, if Manager 1 wants to carry out his activities as *Manager* of his team, he simply uses his user name. As soon as he wants to perform his role as *Payroll Manager*, he needs a second system user (with the respective authorization as in the above example).
The problem is that you will need many users to map the user-specific contexts in your company. This is why the Context Solution has been developed for HR Master Data.

3 Context Solution for HR Master Data

A context-dependent realization of authorizations has been developed in HR Master Data. This required a close interaction between general and structural authorizations, both of which are based on technically different concepts.

The close interaction was achieved by creating a technical connection between general and structural authorization profiles. The new Master Data authorization objects, P_ORGINCON and P_ORGXXCON were developed to make this connection possible. The new authorization objects differ from the old authorization objects P_ORGIN and P_ORGXX in that they contain a new field, PROFL. You can enter structural profiles in this field.



The new authorization objects enable users to perform as many roles as they want to using a single user ID and without causing the current authorization profiles to be overridden.

4 Technical Settings for the Context Solution

This section describes all the technical settings you need for the context solution:

- Maintaining the new authorization objects using the transaction SU21:
  - P_ORGINCON (HR: Master Data with Context)
  - P_ORGXXCON (HR: Extended Check with Context)
  - Customer-specific authorization object for Master Data, P_NNNNCON for the context solution and the corresponding parameterization of the report RPUACG00 (Code Generation: HR Infotype Authorization Check)
- Creating the new Authorization Main Switch using table T77S0:
  - AUTSW INCON
  - AUTSW XXCON
  - AUTSW NNCON
  - AUTSW DFCON

4.1 P_ORGINCON (*HR: Master Data with Context*)

Authorization Object that is used during the authorization check for HR data. This check takes place when HR infotypes are edited or read. You can map user-specific contexts in HR Master Data using P_ORGINCON.

The authorization object P_ORGINCON consists of the same fields as P_ORGIN and has been expanded to include the PROFL field:

Authorization Field	Long Text
INFTY	Infotype
SUBTY	Subtype
AUTHC	Authorization Level
PERSA	Personnel Area
PERSG	Employee Group
PERSK	Employee Subgroup
VDSK1	Organizational Key
PROFL	Authorization Profile

More Information About the Fields

- The AUTHC field contains the access mode for the authorization (for example, **R** = Read). See Authorization Level for a description of the different authorization levels (**M**, **R**, **S**, **E**, **D**, **W**, *****) available.
- The VDSK1 field enables you to run diverse authorization checks by organizational assignment (using the authorization object P_ORGINCON). The content of the organizational key is either derived by the system from the fields of the *Organizational Assignment* infotype (0001) or entered manually by the user.
- The PERSA, PERSG, PERSK, and VDSK1 fields are filled from the *Organizational Assignment* infotype (0001). Since this infotype has time-dependent specifications, an authorization may only exist for certain time intervals depending on the user's authorization.

  Note:

  The time dependency of infotypes is stored in table T582A (*Infotypes – Customer-Specific Settings*) in the VALDT field.

All the time intervals for which a user has authorizations for P_ORGINCON constitute a user's period of responsibility.

- The PROFL field is used to determine which structural profile the user is authorized to access. Note that you can only enter structural profiles in this field that are assigned to the user in table T77UA (*User Authorizations = Assignment of Profile to User*).

In the standard system, the check of this object is not active. You can use the AUTSW INCON authorization main switch to control the use of P_ORGINCON.

4.2 P_ORGXXCON (*HR: Extended Check with Context*)

Authorization Object that is used during the authorization check on HR infotypes. The check takes place when HR infotypes are edited or read. You can map user-specific contexts in HR Master Data using P_ORGXXCON.

The authorization object P_ORGXXCON consists of the same fields as P_ORGXX and has been expanded to include the PROFL field:

Authorization Field	Long Text
INFTY	Infotype
SUBTY	Subtype
AUTHC	Authorization Level
SACHA	Payroll Administrator
SACHP	Master Data Administrator
SACHZ	Time Recording Administrator
SBMOD	Administrator Group
PROFL	Authorization Profile

More Information About the Fields:

- The AUTHC field contains the access mode for the authorization (for example, **R** = Read). See Authorization Level for a description of the different authorization levels (**M**, **R**, **S**, **E**, **D**, **W**, *****) possible.
- The SACHA, SACHP, SACHZ, and SBMOD fields are filled from the *Organizational Assignment* infotype (0001). Since this infotype has time-dependent specifications, an authorization may only exist for certain time intervals depending on the user's authorization. All the time intervals for which a user has authorizations for P_ORGXXCON constitute a user's period of responsibility.
- The PROFL field is used to determine which structural profiles the user is authorized to access. Note that you can only enter structural profiles that are assigned to the user in table T77UA (*User Authorizations = Assignment of Profile to User*) in this field.

In the standard system, the check of this object is not active. You can use the AUTSW XXCON authorization main switch to control the use of P_ORGXXCON.

4.3 P_NNNNNCON (*HR Master Data: Customer-Specific Authorization Object with Context*)

If you have requirements that cannot be mapped using the P_ORGINCON and P_ORGXXCON authorization objects (for example, because you want to build your authorization checks on additional fields of the *Organizational Assignment* infotype (0001) that are customer-specific) and if you want to implement the context solution, you can include an authorization object in the authorization checks yourself.

A customer-specific authorization object for the context solution must contain the following fields:

Authorization Field	Long Text
INFTY	Infotype
SUBTY	Subtype
AUTHC	Authorization Level
PROFL	Authorization Profile

You can use any of the fields in the *Organizational Assignment* infotype (0001) or in the PA0001 structure. You can also use customer-specific additional fields as long as they are CHAR or NUMC type fields.

In addition, you can use the following fields:

- TCD: This field is always filled with the current transaction code (SY-TCODE). Note that when you use this authorization object in reports, the TCD field is filled with the name of the transaction that calls up the report and not with the report name.
- INFSU: This field is 8 characters long. The first 4 characters contain the infotype, the last 4 characters the subtype.

To create a customer-specific authorization object, you can use the RPUACG00 report.

Note:

Note that if you use customer-specific authorization objects, you must maintain these objects in the transaction SU24 in the same way as you maintain the authorization objects P_ORGIN (*HR: Master Data*), P_ORGXX (*HR: Master Data – Extended Check*) and P_PERNR (*HR: Master Data – Check by Personnel Number*).
In the standard system, the check of this object is not active. You can use the AUTSW NNCON authorization main switch to control the use of the customer-specific authorization object.

4.3.1 Report RPUACG00 (*Code Generation: HR Infotype Authorization Check*)

You can use this report to generate the necessary ABAP coding for a customer-specific authorization object that is to be included in the HR infotype authorization check.
If you want to implement the context solution, that is create a customer-specific authorization object that contains the PROFL field, you must select the *With Context Solution* parameter on the report's selection screen.

This generates the ABAP coding for the customer context authorization object that you have just created (using the Include MPPAUTCON).

4.4 New Authorization Main Switches

New Authorization Main Switches of the AUTSW group have been stored in table T77S0 for the context solution. You can use these switches to control the use of the new authorization objects:

- AUTSW INCON
- AUTSW XXCON
- AUTSW NNCON
- AUTSW DFCON

You can edit the settings of the authorization main switch using the transaction OOAC (*HR: Authorization Main Switch*).

Note that you can activate the AUTSW ORGIN main switch (*HR: Master Data*), AUTSW XXCON (*HR Master Data: Extended Check (Context)*) or AUTSW ORGXX (*HR Master Data: Extended Check*), and AUTSW INCON (*HR Master Data (Context)*) simultaneously.

See also:

Recommendations for Setting Up the Authorization Main Switch

4.4.1 AUTSW INCON (*HR Master Data (Context)*)

Authorization Main Switch that controls whether the P_ORGINCON authorization object should be used in the authorization check.

Values:

In the standard system, this switch is set to **0**. If you want to activate the authorization check against P_ORGINCON, set the switch to **1**.

See also:

Recommendations for Setting Up the Authorization Main Switch

4.4.2 AUTSW XXCON (*HR Master Data: Extended Check (Context)*)

Authorization Main Switch that controls whether the P_ORGXXCON authorization object should be used in the authorization check.

Values:

In the standard system, this switch is set to **0**. If you want to activate the authorization check against P_ORGXXCON, set the switch to **1**.

See also:

Recommendations for Setting Up the Authorization Main Switch

4.4.3 AUTSW NNCON (*Customer Authorization Object (Context)*)

Authorization Main Switch that controls whether the P_NNNNNCON customer-specific authorization object should be used in the authorization check.

Values:

In the standard system, this switch is set to **0**. If you want to activate the authorization check against P_NNNNNCON, set the switch to **1**.

See also:

Recommendations for Setting Up the Authorization Main Switch

4.4.4 AUTSW DFCON (*Authorization Check for a Person with Default Position*)

Authorization Main Switch that controls how the system should react, if the context solution is set up, to personnel numbers that are not linked to the organizational structure (in other words, personnel numbers that have position entered as the default position in the *Organizational Assignment* infotype (0001)).

Values:

In the Standard System, this switch is set to **1.** You can set the switch to **1**, **2**, **3** or **4**. The different switch settings specify how the system should react to personnel numbers that are not linked to the organizational structure (in other words, personnel numbers that have position entered as the default position in the *Organizational Assignment* infotype (0001)).

For these personnel numbers, you may want to refer to the organizational unit stored in the *Organizational Assignment* infotype (0001) for the authorization check (if the organizational unit exists). If you want to do so, you must set the main switch to **1** or **3**, otherwise to **2** or **4**. If the person is assigned the default position and no organizational unit is specified in the *Organizational Assignment* infotype (0001), which means that it should not be evaluated, no authorization check by organizational assignment can take place.

In this case, you can specify in the settings whether the system should grant or deny the authorization by default. If you want to deny the authorization by default, set the main switch to **1** or **2**, otherwise to **3** or **4**. The following combinations are possible for the switch settings:

	Evaluate organizational unit (if available)	**Never evaluate organizational unit**
Deny authorization by default	**1**	**2**
Grant authorization by default	**3**	**4**

Note:

You can make this setting for non-context authorization objects using the AUTSW ORGPD switch.

4.4.5 Recommendations for Setting Up Authorization Main Switches

This section provides you with suggestions on how best to set up the new authorization main switches if you implement the context solution.

1. **You implement the context solution for all authorization objects:**

INCON	on	ORGPD	off	ORGIN	off
XXCON	on			ORGXX	off
NNCON	on			NNNNN	off

2. **You implement a combination of context authorization object and non-context authorization object, for example, ORGINCON and ORGXX:**

INCON	on	ORGPD	on	ORGIN	off
XXCON	off			ORGXX	on
NNCON	off/on			NNNNN	off/on

5 Glossary

Evaluation Path

Chain of relationships that exists between objects in a hierarchical structure.
The evaluation path O-S-P, for example, describes the relationship chain organizational unit → position → person.
Evaluation paths are used, for example, to select objects during evaluations. You choose an evaluation path and the system evaluates the structure along this evaluation path. The report takes account only of the objects that lie along the specified evaluation path.

Authorization

Authority to carry out a particular activity in the system.
An authorization is granted for a specific authorization object and is stored in the user master record of a user. You can think of an authorization as a key that fits the locks of a specific lock system (to build up the authorization object).
Just as there are master keys and general keys to the locks in a lock system, there are authorizations, which enable authorization checks to exist. The authorizations and checks must, however, always belong to the same authorization object (that is to the same key system).

Authorization Object

Technical tool used to carry out authorization checks.
From a system point of view, an authorization object primarily determines the technical context for the authorization check. In other words, which fields with which field specifications the system should consider during the corresponding authorization check. You can specify a maximum of ten fields per authorization object. The actual check and the business meaning of this check are determined by a program of the corresponding application.
You can think of an authorization object as the building instructions for the locksmith of a lock system. The object does not determine which authorizations you need at a position (which keys fit in which locks), instead it determines which fields are used as part of the authorization check (what the keys or locks look like). In addition, the object does not determine which programs access it (where a lock is built) and how the programs react after the corresponding authorization checks (what happens when you turn the key).

Authorization Main Switch

Collective term for the AUTSW group entries from table T77S0 (*System Table*) that are connected with HR authorizations. You can generally control the use of an authorization object during the authorization check using this switch.
Example:
The ORGIN entry controls the use of the P_ORGIN authorization object.

Authorization Level

AUTHC field in master data authorization objects that contains the access mode by which a user gains access to system data.
Possible specifications of an authorization level are:

M: Read entry helps

R: Read

E: Write locked data records

D: Maintain lock indicators

W: Write data records

***:** All operations

Authorization Profile

Grouping of authorizations. Analogy: Bunch of keys (where a key = an authorization)

Authorization Check

Point in the program at which the system asks for a specific authorization. You can think of the authorization check as the lock to a lock system.

Overall Profile

All the authorization profiles from general and structural authorizations that a user has in the system.

Role

Group of activities that a user with a specific task profile carries out.
A role is defined by the transactions, reports, web-based applications and so on that it contains. User menus provide access to the activities contained in roles.

Role Maintenance

You can use the transaction PFCG to define, generate, and assign roles and the menus and authorization profiles belonging to roles.

*-Entry

Input value that you can enter instead of concrete values when assigning authorizations.
A ***** can substitute any value. If **XY*** is entered in a field as part of an authorization, the corresponding authorization check will be successful for **XY**, **XYA**, **XYB**, **XYZ**, **XY1**, for example, but not for **ABC**. If ***** is entered in a field, the corresponding authorization check will always be successful.

Copyright