



An Expert Guide to New SAP BI Security Features

Marc Bernard
SAP Labs

In this session you will ...

- Learn how to grant access to data on various levels of detail
- Find out how the new analysis authorizations compare to the old concept based on authorization objects
- Understand the new options for defining authorizations
- See a demonstration of the new functionality
- Hear about migration tools
- Take away information about the latest monitoring and auditing capabilities for security settings



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

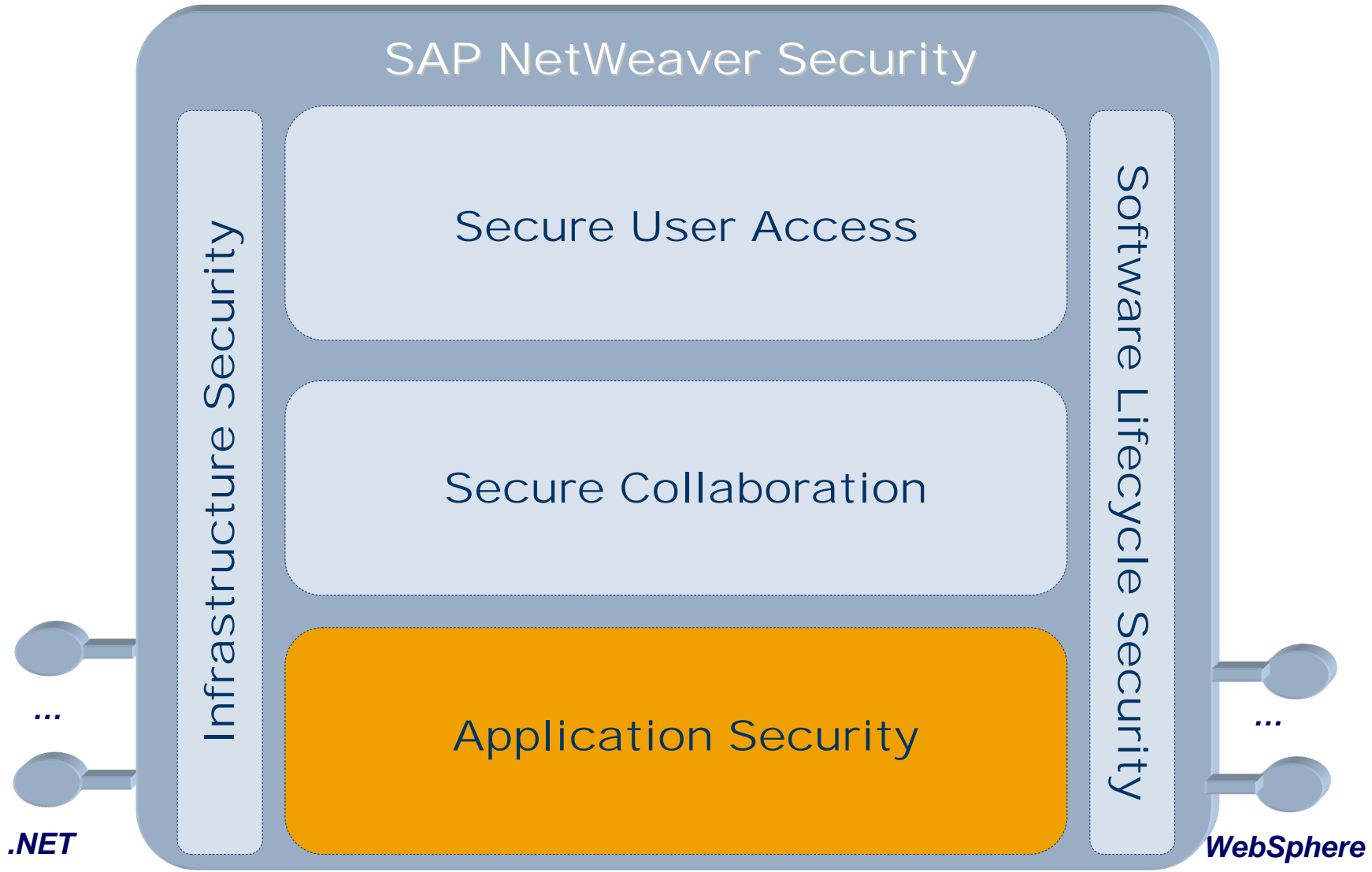
Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

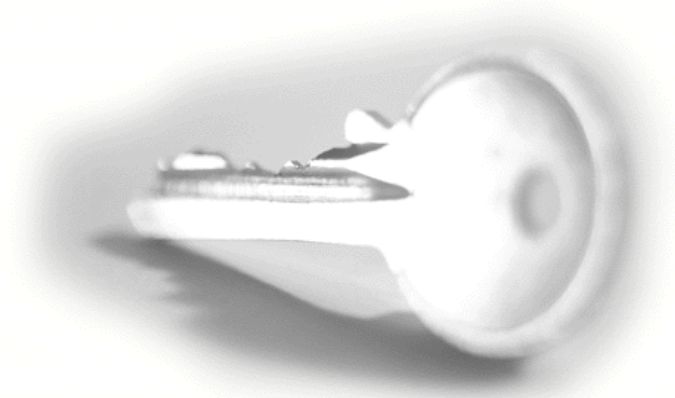
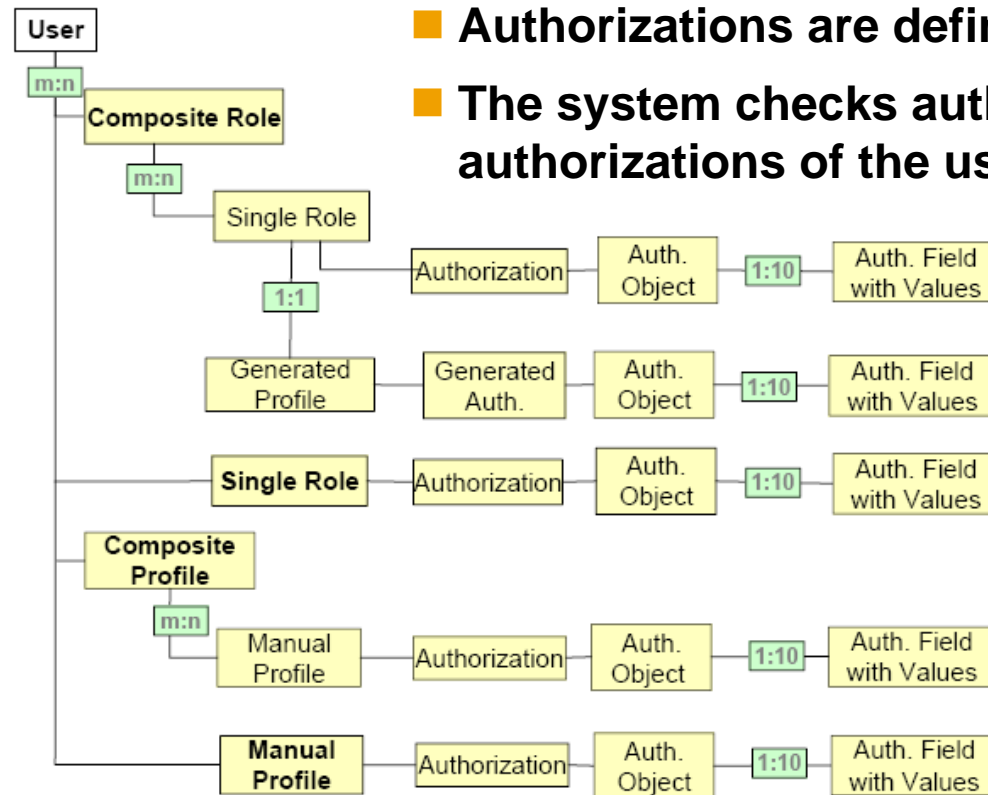
Migration

Summary



Application Security

- Based on **roles and authorization** concept
- Users are assigned to roles
- Roles contain authorizations
- Authorizations are defined for **authorization objects**
- The system checks authorization objects against the authorizations of the user



Security Needs in mySAP ERP (OLTP)

- **Transaction-based security**
- **Driven by:**
 - ◆ **Transaction codes**
 - ◆ **Specific field values**
 - ◆ **Which activities a user can perform**
- **Focused on getting daily work completed as quickly and efficiently as possible**

Security Needs in SAP NetWeaver BI (OLAP)

- **Analysis-based security**
- **Driven by:**
 - ◆ **InfoProviders**
 - ◆ **Queries**
 - ◆ **Data**
- **Different business purpose and goals than OLTP**
- **Focused on displaying, planning, and analyzing data**

Standard Authorizations

- Based on standard role and authorization concept of SAP
- Was and still are used for BI administrator and developer activities

Reporting Authorizations

- Old security concept up to SAP NetWeaver '04 (up to SAP BW 3.5)
- Control for which data a user has access to in a query
- Realized through the standard authorization concept, which has many limitations

Analysis Authorizations

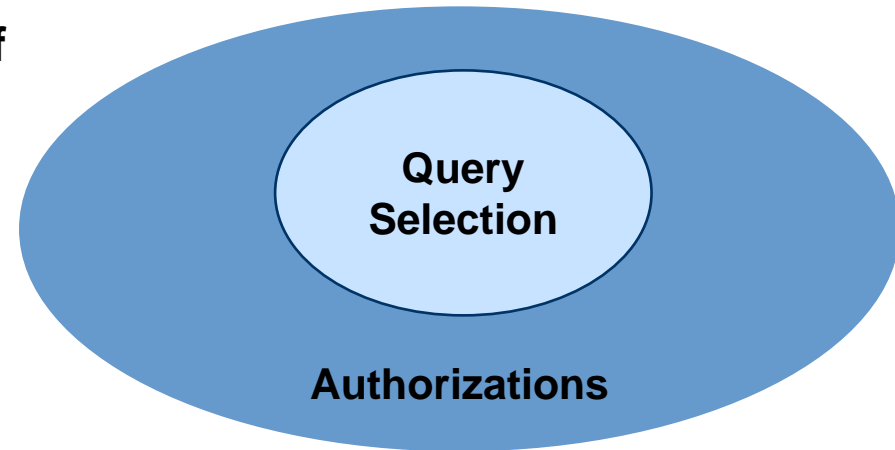
- New security concept as of SAP NetWeaver 2004s
- Is not based on standard authorization concept in order to overcome the limitations
- Takes features of reporting and analysis in BI into consideration



Covered in
this presentation

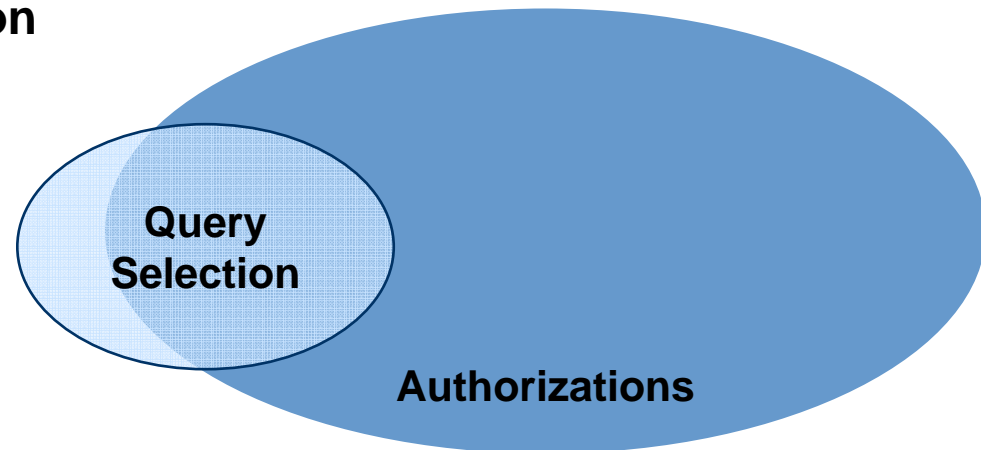
Scenario: Sufficient Authorizations

- Complete selection is subset of authorizations
- Query results will be shown



Scenario: Insufficient Authorizations

- Complete or part of selection is outside of authorizations
- Query results will not be shown at all



Exceptions for “All-or-Nothing” Rule

- **Display hierarchies are automatically filtered by the authorization**
- **Key figure values are not displayed if the key figure is not authorized**

Authorization Levels

Access Can Be Restricted by Authorizations ...

- On InfoCube Level
- On Characteristic Level
- On Characteristic Value Level
- On Key Figure Level
- On Hierarchy Node Level

■ On Characteristic Level

Top customers (Drag&Relate) Validity of Data: 10.02.2005 15:54:11

Sold-to party	Sales	Cost of sales	DB 1	DB 1 (%)
Elektromarkt Bamby	28,791 EUR	15,835 EUR	12,956 EUR	45.0 %
J & P	26,815 EUR	13,328 EUR	13,487 EUR	50.3 %
Motomarkt Stuttgart GmbH	24,761 EUR	14,180 EUR	10,581 EUR	42.7 %
Lampen-Markt GmbH	20,927 EUR	12,128 EUR	8,799 EUR	42.0 %
Christal Clear	20,262 EUR	11,974 EUR	8,288 EUR	40.9 %
Motor Sports	19,205 EUR	9,941 EUR	9,263 EUR	48.2 %
Motomarkt Heidelberg GmbH	18,136 EUR	7,344 EUR	10,792 EUR	59.5 %
SudaTech GmbH	17,503 EUR	12,440 EUR	5,062 EUR	28.9 %
Karsson High Tech Markt	17,031 EUR	11,766 EUR	5,245 EUR	30.8 %
HTG Komponente GmbH	16,312 EUR	11,759 EUR	4,553 EUR	27.9 %
N.I.C. High Tech	16,231 EUR	11,634 EUR	4,597 EUR	28.3 %
Carbor GmbH	16,192 EUR	3,527 EUR	12,665 EUR	78.2 %
Overall Result	462,282 EUR	249,394 EUR	212,888 EUR	46.4 % MXD

■ On Characteristic Value Level

Top customers (Drag&Relate) Validity of Data: 10.02.2005 15:54:11

Sold-to party	Sales	Cost of sales	DB 1	DB 1 (%)
Elektromarkt Bamby	28,791 EUR	15,835 EUR	12,956 EUR	45.0 %
J & P	26,815 EUR	13,328 EUR	13,487 EUR	50.3 %
Motomarkt Stuttgart GmbH	24,761 EUR	14,180 EUR	10,581 EUR	42.7 %
Lampen-Markt GmbH	20,927 EUR	12,128 EUR	8,799 EUR	42.0 %
Christal Clear	20,262 EUR	11,974 EUR	8,288 EUR	40.9 %
Motor Sports	19,205 EUR	9,941 EUR	9,263 EUR	48.2 %
Motomarkt Heidelberg GmbH	18,136 EUR	7,344 EUR	10,792 EUR	59.5 %
SudaTech GmbH	17,503 EUR	12,440 EUR	5,062 EUR	28.9 %
Karsson High Tech Markt	17,031 EUR	11,766 EUR	5,245 EUR	30.8 %
HTG Komponente GmbH	16,312 EUR	11,759 EUR	4,553 EUR	27.9 %
N.I.C. High Tech	16,231 EUR	11,634 EUR	4,597 EUR	28.3 %
Carbor GmbH	16,192 EUR	3,527 EUR	12,665 EUR	78.2 %
Overall Result	462,282 EUR	249,394 EUR	212,888 EUR	46.4 % MXD

■ On Key Figure Level

Top customers (Drag&Relate) Validity of Data: 10.02.2005 15:54:11

Sold-to party	Sales	Cost of sales	DB 1	DB 1 (%)
Elektromarkt Bamby	28,791 EUR	15,835 EUR	12,956 EUR	45.0 %
J & P	26,815 EUR	13,328 EUR	13,487 EUR	50.3 %
Motomarkt Stuttgart GmbH	24,761 EUR	14,180 EUR	10,581 EUR	42.7 %
Lampen-Markt GmbH	20,927 EUR	12,128 EUR	8,799 EUR	42.0 %
Christal Clear	20,262 EUR	11,974 EUR	8,288 EUR	40.9 %
Motor Sports	19,205 EUR	9,941 EUR	9,263 EUR	48.2 %
Motomarkt Heidelberg GmbH	18,136 EUR	7,344 EUR	10,792 EUR	59.5 %
SudaTech GmbH	17,503 EUR	12,440 EUR	5,062 EUR	28.9 %
Karsson High Tech Markt	17,031 EUR	11,766 EUR	5,245 EUR	30.8 %
HTG Komponente GmbH	16,312 EUR	11,759 EUR	4,553 EUR	27.9 %
N.I.C. High Tech	16,231 EUR	11,634 EUR	4,597 EUR	28.3 %
Carbor GmbH	16,192 EUR	3,527 EUR	12,665 EUR	78.2 %
Overall Result	462,282 EUR	249,394 EUR	212,888 EUR	46.4 % MXD



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing and Test Tools

Migration

Summary

Comparing Authorization Concepts

Limitations of earlier SAP BW releases

	<=SAP BW 3.x
Technical Foundation	Authorization objects
Maintenance	Not changeable afterwards
Number of InfoObjects	Ten InfoObjects
Navigational Attributes	Only on global basis
Hierarchy Authorizations	Via GUID and OTCTAUTHH
Composition of Authorizations	Only intersection of auth. objects permitted
Authorization Relevance	Per InfoObject AND InfoCube
Validity	Tied to role only
InfoProvider Authorizations	Separate authorization objects (S_RS_*)

Comparing Authorization Concepts (cont.)

Improvements with SAP NetWeaver 2004s

	<=SAP BW 3.x	SAP NetWeaver 2004s
Technical Foundation	Authorization objects	Analysis authorization
Maintenance	Not changeable afterwards	Changeable
Number of InfoObjects	Ten InfoObjects	Number of InfoObjects not limited
Navigational Attributes	Only on global basis	Individually
Hierarchy Authorizations	Via GUID and OTCTAUTHH	Equivalent to value authorizations
Composition of Authorizations	Only intersection of auth. objects permitted	Union "as expected"
Authorization Relevance	Per InfoObject AND InfoCube	Only InfoObject setting
Validity	Tied to role only	Flexible per authorization
InfoProvider Authorizations	Separate authorization objects (S_RS_*)	Included in authorization

**Please see the appendix on your take-home CD
for a detailed comparison**



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary

Follow these steps to create your authorizations

InfoObject Maintenance (RSD1):

- 1. Define Authorization-Relevant Characteristics**
- 2. Define Authorization-Relevant Attributes**

Management of Analysis Authorizations (RSECADMIN):

- 3. Authorize Characteristic Values**
- 4. Authorize Attribute Values**
- 5. Authorize Hierarchies**
- 6. Add Special Authorization Characteristics**
- 7. Add Key Figure Authorizations**
- 8. Add Variables in Authorizations**

Business Content for Authorizations

Before you get started, here are some tips:

- **Activate all Business Content related to authorizations before you get started**
 - ◆ InfoObjects: 0TCA* (and 0TCT* if not done already)
 - ◆ InfoCubes: 0TCA*
- **Set the following InfoObjects as “authorization-relevant”**
 - ◆ 0TCAACTVT
 - ◆ 0TCAIPROV
 - ◆ 0TCAVALID
 - ◆ 0TCAKYFNM
- **Add 0TCAIFAREA as an external hierarchy characteristic to 0INFOPROV**

Data Warehousing Workbench: Business Content

Collected objects	I	M	S	A	Technical name	Elevated o...	BC...	Co...	Last	Person r...
<input type="checkbox"/>					Change Document Analysis Author	<input type="checkbox"/>				
<input type="checkbox"/>					0TCA_HIE	<input checked="" type="checkbox"/>		7.0/...	18.01...	SAP
<input type="checkbox"/>					Change Document Authorizations	<input type="checkbox"/>				
<input type="checkbox"/>					0TCA_UA	<input checked="" type="checkbox"/>				SAP
<input type="checkbox"/>					Change Document Analysis Author	<input type="checkbox"/>		7.0/...	18.01...	SAP
<input type="checkbox"/>					0TCA_VAL	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Activity in Analysis Authorizations	<input type="checkbox"/>		7.0/...	16.02...	SAP
<input type="checkbox"/>					0TCAACTVT	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Number of Authorization Records	<input type="checkbox"/>		7.0/...	18.01...	SAP
<input type="checkbox"/>					0TCAccount	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					InfoArea for Analysis Authorizations	<input type="checkbox"/>		7.0/...	01.03...	SAP
<input type="checkbox"/>					0TCAIFAREA	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Authorizations for InfoProvider	<input type="checkbox"/>		7.0/...	16.02...	SAP
<input type="checkbox"/>					0TCAIPROV	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Key Figure in Analysis Authorization	<input type="checkbox"/>		7.0/...	16.06...	SAP
<input type="checkbox"/>					0TCAKYFNM	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Authorizations Language	<input type="checkbox"/>		22.09...		SAP
<input type="checkbox"/>					0TCALANG	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Language of Authorization Texts	<input type="checkbox"/>		22.09...		SAP
<input type="checkbox"/>					0TCALANGU	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Change Type Analysis Authorizator	<input type="checkbox"/>		7.0/...	18.01...	SAP
<input type="checkbox"/>					0TCARecMODE	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Texts Load Authorizations	<input type="checkbox"/>		22.09...		SAP
<input type="checkbox"/>					0TCAXTLG	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Texts Load Authorizations	<input type="checkbox"/>		22.09...		SAP
<input type="checkbox"/>					0TCAXTMD	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Texts Load Authorizations	<input type="checkbox"/>		22.09...		SAP
<input type="checkbox"/>					0TCAXTSH	<input checked="" type="checkbox"/>				
<input type="checkbox"/>					Validity of an Authorization	<input type="checkbox"/>		7.0/...	16.02...	SAP
<input type="checkbox"/>					0TCAVALID	<input checked="" type="checkbox"/>				

1. Authorization-Relevant Characteristics

Before restricting authorizations on characteristics, you have to mark them as authorization-relevant

Change Characteristic 0D_SALE_ORG: Detail

Characteristic: 0D_SALE_ORG
Long description: Sales Organization (SAP Demo)
Short description: Sales organization
Version: Revised (Not saved)
Object Status: Active, executable

General | Business Explorer | Master data/texts | Hierarchy | Attribute

General settings

Display	Key and Text
Text Type	Default
BEx description	Short description
Selection	No Selection Restriction
Query Def. Filter Value Selection	Values in Master Data Table
Query Execution Filter Val. Selectn	Only Posted Values for Navigation
Base Unit of Measure	
Units of Measure for Char.	
Currency attribute	
<input checked="" type="checkbox"/> AuthorizationRelevant	

BEx Map

Geographical type	Static geo-characteristic
Geographical attribute	

Upload Shapefiles | Edit shape files | Geo Data Download (Everything) | GeoData Download (Delta)

InfoObject Maintenance (Transaction RSD1)

2. Authorizing Navigational Attributes

If you want to grant authorizations on navigational attributes, mark them in the attribute tab strip as authorization-relevant

Change Characteristic 0D_SALE_ORG: Detail

← → [Icons] Maintain Logs... Metadata

Version Comparison Business Content

Characteristic: 0D_SALE_ORG

Long description: Sales Organization (SAP Demo)

Short description: Sales organization

Version: Active Saved

Object Status: Active, executable

Business Explorer Master data/texts Hierarchy Attribute Com...

Assigned DataSource Attributes Navigation Attribute InfoProvider

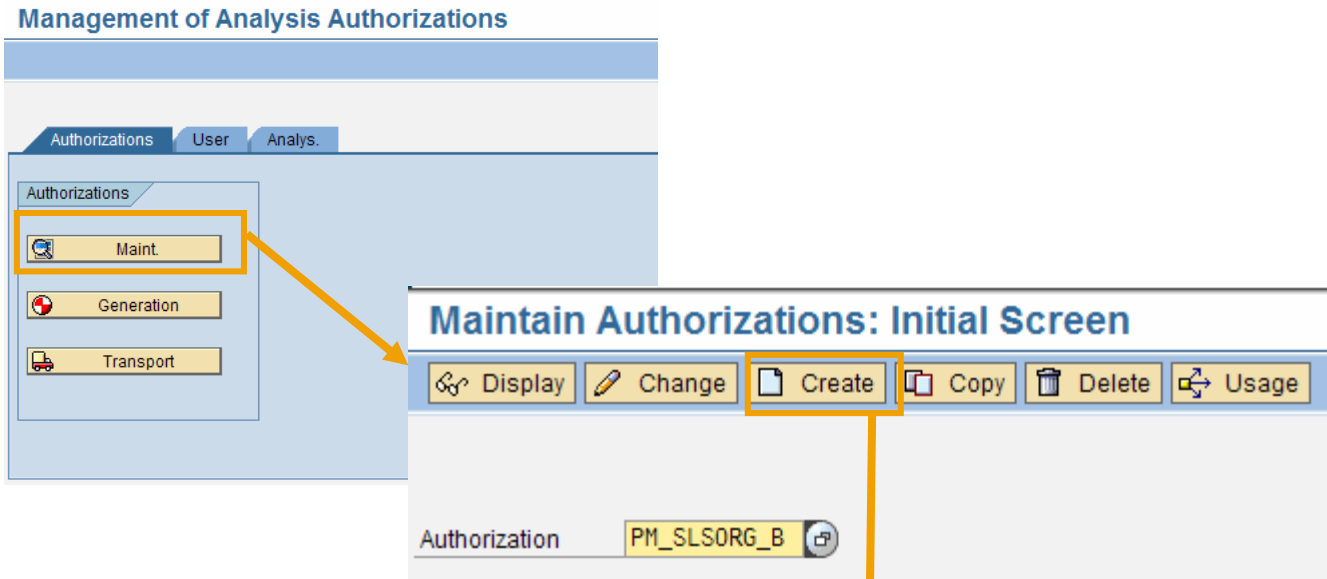
Attributes: Detail/Navigation Attributes

Attribute	Long description	Ty.	Ti	Or.	N	Aut	T	Navigation att. desc
0D_COUNTRY	Country (SAP Demo)	NAV	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Country (SAP Demc
			<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
			<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
			<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
			<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
			<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

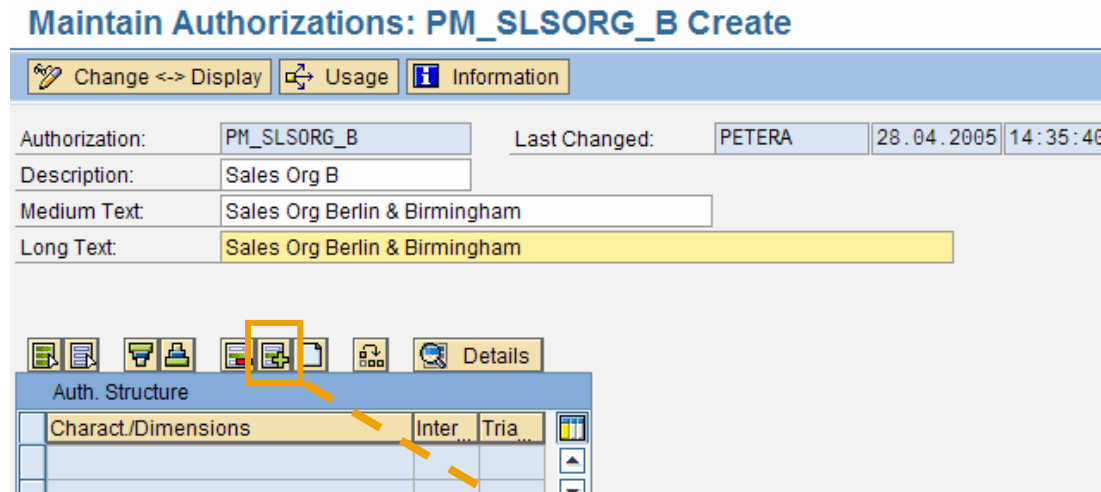
InfoObject Maintenance (Transaction RSD1)

3. Authorizing Characteristic Values

Central maintenance for (analysis) authorizations/ transaction RSECADMIN

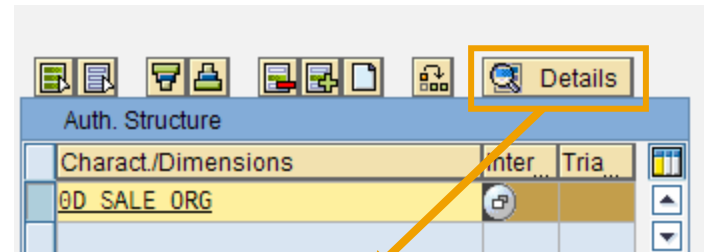


Scenario: A group of users is authorized only to specific sales organizations (e.g., Berlin and Birmingham)

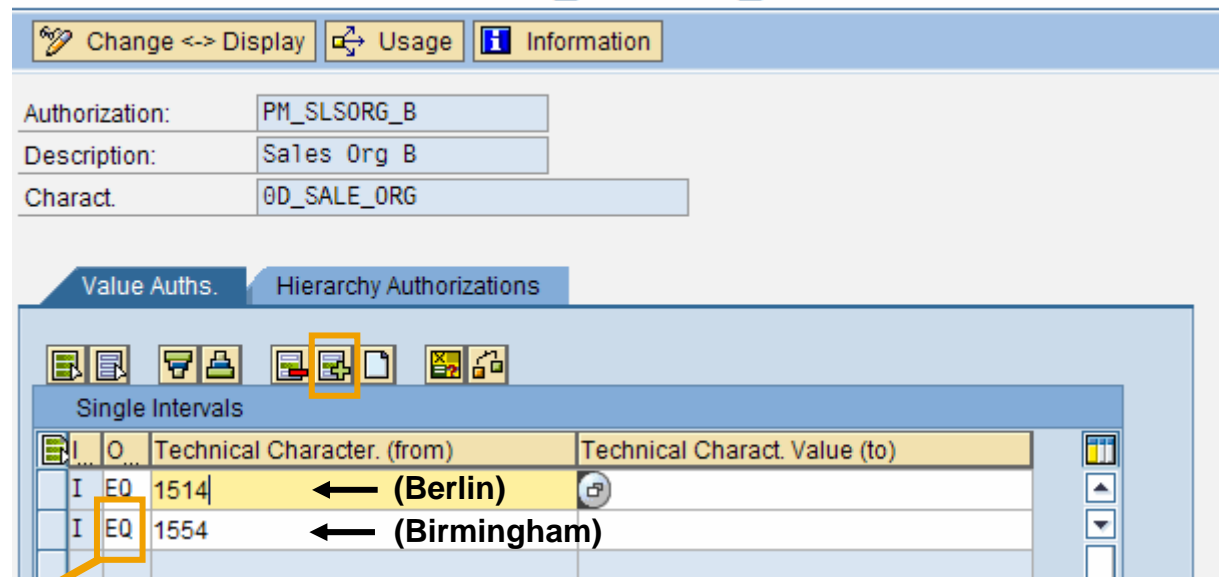


3. Authorizing Characteristic Values (cont.)

A group of users is authorized only to specific sales organizations (e.g., Berlin and Birmingham)



Maintain Authorizations: PM_SLSORG_B Create



Possible Values

- EQ: Single value
- BT: Range of values
- CP: Contains (simple) patterns ending with * (e.g., XY*)

Special Authorization Value

Special Authorization Values (for all characteristics)

* (asterisk)

- Denotes a set of arbitrary characters
- Used alone to grant access to **all values**
- Used at the end of a value to specify a simple pattern (example: SAP*)

: (colon)

- Allows access only to **aggregated data** (e.g., allows information on all sales areas only on aggregated level – not on particular sales areas)

+ (plus)

- Denotes exactly one character
- Used at the end of a value to specify a simple pattern (example: RED+)
- Used to specify **date patterns** (only for Validity (0TCAVALID))

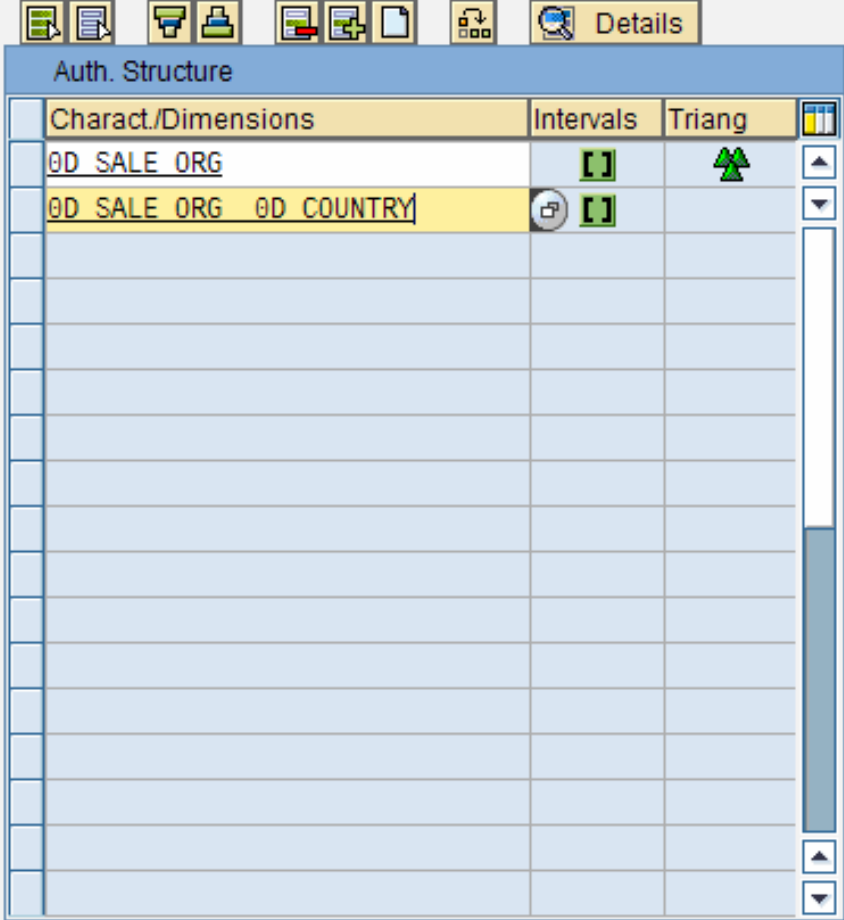
(hash)

- Stands for the **initial or unassigned value**

4. Authorizing Navigational Attributes

Navigational Attributes

- Can be assigned individually
- Tip: The referencing characteristic (here: 0D_SALE_ORG) does not need to be authorization-relevant



The screenshot shows the 'Auth. Structure' table in SAP. The table has three columns: 'Charact./Dimensions', 'Intervals', and 'Triang'. The first row is highlighted in yellow and contains '0D_SALE_ORG' in the 'Charact./Dimensions' column, a green square icon in the 'Intervals' column, and a green tree icon in the 'Triang' column. The second row is also highlighted in yellow and contains '0D_SALE_ORG 0D_COUNTRY' in the 'Charact./Dimensions' column, a green square icon in the 'Intervals' column, and an empty cell in the 'Triang' column. The table is part of a larger interface with a toolbar at the top and a 'Details' button.

Charact./Dimensions	Intervals	Triang
0D_SALE_ORG	[]	[]
0D_SALE_ORG 0D_COUNTRY	[]	

5. Authorizing Hierarchies

In the same way as with value authorization, you can also grant authorizations on hierarchy levels

Assume you'll have a sales organization as depicted

Hierarchy 'Sales Organisation' Change: 'Modified Version'

The screenshot displays the SAP Hierarchy Editor interface. The title bar reads "Hierarchy 'Sales Organisation' Change: 'Modified Version'". The toolbar includes icons for "Maintain Level", "Hierarchy Attributes", and "Interval". The main window shows a tree structure for "Sales Organisation". The "Global Sales" node is selected and highlighted in yellow. Under "Global Sales", there are four main regional nodes: "Americas", "Europe", "United Kingdom", and "Germany". Each regional node contains a list of specific locations, each with a small green triangle icon. The "Americas" region includes "USA" (with sub-nodes: New York, San Francisco, Illinois, Colorado, Alaska) and "Canada" (with sub-nodes: Toronto, Vancouver). The "Europe" region includes "United Kingdom" (with sub-nodes: London, Birmingham), "France" (with sub-nodes: Paris, Marseille, Grenoble), and "Germany" (with sub-nodes: Frankfurt, Berlin, Munich, Hamburg).

5. Authorizing Hierarchies (cont.)

Now you grant access for the complete Americas and France

Maintain Authorizations: PM_SLSORG_B Create

Change <-> Display Usage Information

Authorization: PM_SLSORG_B
Description: Sales Org B
Charact. @D_SALE_ORG

Value Auths. Hierarchy Authorizations

Create Details

Hierarchy Name	Technical Node Name	Ty	Hi	Ar
PM_SALE_ORG	PM_AMERICA	1	0	
PM_SALE_ORG	PM_FRANCE	1	0	

Maintain Authorizations: PM_SLSORG_B Create

Definition of Hierarchy Authorization

Hierarchy PM_SALE_ORG/99991231//@D_SALE_ORG
Nodes PM_FRANCE

Type of Authorization 1
Subtree Below Nodes

Hierarchy Level 0
Validity Period

Name, Version Identical and Key Date Less Than or Equal to

✓ ✗

You can also use variables to flexibly and dynamically determine hierarchy nodes

5. Authorizing Hierarchies (cont.)

Maintain Authorizations: PM_SLSORG_B Create

Definition of Hierarchy Authorization

Hierarchy PM_SALE_ORG/99991231//0D_SALE_ORG

Nodes PM_FRANCE

Type of Authorization 1

Subtree Below Nodes

Hierarchy Level 0

Validity Period

Name, Version Identical and Key Date Less Than or Equal to

Type of Authorization

- Only the selected nodes
- Subtree below nodes
- Subtree below nodes to level (incl.)
- Complete hierarchy
- Subtree below nodes to (and including) level (relative)

→ Use case: Hierarchies that happen to be restructured regularly

5. Authorizing Hierarchies (cont.)

Maintain Authorizations: PM_SLSORG_B Create

Definition of Hierarchy Authorization

Hierarchy PM_SALE_ORG/99991231//0D_SALE_ORG

Nodes PM_FRANCE

Type of Authorization 1

Subtree Below Nodes

Hierarchy Level 0

Validity Period

Name, Version Identical and Key Date Less Than or Equal to

Validity Range

Which authorization hierarchy is checked against the currently used hierarchy (strictness of check)?

- Name, Version Identical, and Key Date Less Than or Equal to
- Name and Version Identical
- Name Identical
- All Hierarchies

Recommendation: Try to be as strict as possible!

6. Special Authorization Characteristics

Authorizations on Special Characteristics

Some special characteristics can be included in an authorization.

Note: They must not be included in queries!

These special characteristics must be assigned to a user in at least one authorization

- InfoProvider
- Validity
- Activity

Insert special characteristics

The screenshot shows the SAP 'Maintain Authorizations: PM_SLSORG_B Edit' interface. The 'Auth. Structure' table is visible, listing special characteristics. An orange box highlights the 'Insert' icon in the toolbar, with an arrow pointing to the text 'Insert special characteristics'.

Charact./Dimensions	Inter...	Tria...
@D_SALE_ORG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
@TCAACTVI	<input checked="" type="checkbox"/>	<input type="checkbox"/>
@TCAIPROV	<input checked="" type="checkbox"/>	<input type="checkbox"/>
@TCAVALID	<input checked="" type="checkbox"/>	<input type="checkbox"/>

6. Special Authorization Characteristics (cont.)

Recommendation

It is not technically necessary to include these special characteristics in every authorization, but it is considered a best practice in order to retain clarity

6. Special Authorization Characteristics (cont.)

InfoProvider

- Grant authorization to particular InfoProviders
- Technical name: 0TCAIPROV
- Possible values:
 - Single value (EQ) One InfoProvider
 - Range (BT) Range of InfoProviders
 - Pattern (CP) Selection of InfoProviders (e.g., 0SD_*)
 - Hierarchy node Selection of InfoProviders based on InfoArea hierarchy

- Default

*

All InfoProviders

Maintain Authorizations: TMB_AUTH Create

Change <-> Display Usage Information

Authorization: TMB_AUTH
Description: Special Fields
Charact.: 0TCAIPROV

Value Auths. Hierarchy Authorizations

Single Intervals

I	O	Technical Character. (from)	Technical Charact. Value (to)
I	EQ	0FIGL_C01	
I	BT	0SD_C11	0SD_C13
I	CP	0QM*	

6. Special Authorization Characteristics (cont.)

Validity

- Define when authorizations are valid or not valid

- Technical name: 0TCAVALID

- Possible values

Include (I)	Grant authorization
Exclude (E)	Deny authorization ^
Single value (EQ)	Exactly one date
Range (BT)	Range of dates
Less or Equal (LE)	Everything <= value in FROM field ^
Greater Than (GT)	Everything > value in FROM field ^
Greater or Equal (GE)	Everything >= value in FROM field ^
Less Than (LT)	Everything < value in FROM field ^
Pattern (CP)	Selection of dates ^

+ (plus) denotes exactly one character (e.g., 01.++.2005 until 10.++.2005: allows access only the first 10 days of each month in 2005)

- Default

* Always valid

^ Exclude (E), special ranges (LE, GT, GE, LT), and the plus pattern (+) work ONLY for this special characteristic!

6. Special Authorization Characteristics (cont.)

Activity

- **Grant authorization to different activities**
- **Technical name: 0TCAACTVT**
- **Possible values:**
 - 02** **Change data (for example, for business planning)**
 - 03** **Display data**
- **Default**
 - 03** **Display data**

Maintain Authorizations: TMB_AUTH Create

Change <-> Display Usage Information

Authorization: TMB_AUTH
Description: Special Fields
Charact.: 0TCAACTVT

Value Auths. Hierarchy Authorizations

Single Intervals

I...	O...	Technical Character. (from)	Technical Charact. Value (to)
I	EQ	02	
I	EQ	03	

7. Key Figure Authorizations

Key Figure Authorizations

- **Grant authorization to particular key figures**
- **Technical name: 0TCAKYFNM**
- **Possible values**

Single value (EQ)	Exactly one key figure
Range (BT)	Selection of key figures
Pattern (CP)	Selection of key figures based on pattern
- **Default**

*	All key figures
---	-----------------
- **Tip:** If a particular key figure is defined as authorization-relevant, it will be checked for every InfoProvider



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary

Follow these steps to generate authorizations automatically:

Data Warehouse Workbench (RSA1):

- 1. Activate Business Content**
- 2. Load DataStore Objects**

Management of Analysis Authorizations (RSECADMIN):

- 3. Generate Authorizations**
- 4. View Generation Log**






Tip: Especially with high user counts or very detailed authorizations, generating authorizations will save a lot of manual work

1. Activate Business Content




Business Content for Authorizations

- **SAP delivers Business Content for storing authorizations and user assignment of authorizations**

- **Human Resources (HR)**

ID	Obj. Name	Long Description
 0TCA_DS01		Template for ODS with Authorization Data (Values)
 0TCA_DS02		Template for ODS with Authorization Data (Hierarchy)
 0TCA_DS03		Template for ODS with Description Text Authorizations
 0TCA_DS04		Template for ODS with Assignment of User Authorization
 0TCA_DS05		Template for ODS for Generating Users for Authorizations

- **Controlling (CO)**

ID	Obj. Name	Long Description
 0CCA_001		CO-OM-CCA: User Authorizations (Single Values)
 0CCA_002		CO-OM-CCA: User Authorizations (Hierarchy Nodes)
 0CCA_003		CO-OM-CCA: User for Reporting

2. Load DataStore Objects

DataStore Objects for Authorizations

- Fill the DataStore objects with the user data and authorizations
- Extract the data, for example, from an SAP R/3 source system
or
- Load the data from a flat file

Tip: You might want to add some consistency checks here to avoid errors during the generation later

3. Generate Authorizations

Generation of Authorizations from DataStore Objects

- Start the generation by specifying the relevant DataStore objects

Management of Analysis Authorizations

The screenshot shows the 'Management of Analysis Authorizations' interface. At the top, there are three tabs: 'Authorizations', 'User', and 'Analys.'. Below the tabs, there is a sidebar with three buttons: 'Maint.', 'Generation', and 'Transport'. The 'Generation' button is highlighted with a yellow border. The main area of the interface is currently empty.

Generating Authorizations in BI from Data in the InfoProviders

Logs

DS Objects with Authorization Data for:

Flat Authorizations	OTCA_DS01
Hierarchy Authorizations	OTCA_DS02
Authorization Texts	OTCA_DS03
Authorized User Assignment	OTCA_DS04
User to Be Generated	OTCA_DS05

Start Generation

4. View Generation Log

After the generation is complete, you can view a detailed log

- First check errors, then also look at warnings

Management of Analysis Authorizations

The screenshot displays the 'Management of Analysis Authorizations' interface. On the left, the 'Analysis Tools' sidebar contains buttons for 'Execution as...', 'Error Logs', and 'Generation Logs'. The 'Generation Logs' button is highlighted with a red box, and an orange arrow points from it to the log entry for 'Generation for user TEST1:'. The main window, titled 'Display logs', shows a table of log entries with columns: Date/Time/User, Numb, External ID, Object txt, Sub-object text, Tran, Program, and Mode. The log entries include:

Date/Time/User	Numb	External ID	Object txt	Sub-object text	Tran	Program	Mode
▶ [Success] Checking user (existence in the system...)	6						
▶ [Success] Checking InfoObjects/fields (existence in the systems...)	2						
▼ [Error] Generation of authorizations	10						
▶ [Error] Generation for user TEST1:	3						
▶ [Error] Generation for user TEST2:	2						
▶ [Success] Generation for user TEST3:	1						
▶ [Success] Generation for user TEST4:	1						
▶ [Success] Generation for user TEST5:	1						
▶ [Success] The generation of the authorization was successful	1						
▶ [Success] Assignment of authorizations to users	11						
▼ [Success] 06.10.2004 16:54:58 MUELLERC	16	BI AS Berechtigun	Authorization Gen	GENERATE	SEU_INT	CL_RSO_APIDialog pr	
▼ [Success] Generation of authorizations for DataStore object: AUT_DS01, , ,	3						
▼ [Success] Reading the authorization data from DataStore object AUT_DS01	2						
▶ [Success] The authorizion data was read successfully from DataStore ot:	1						
▶ [Success] Generation of authorizations for InfoProvider group AUT_DS0	13						
▶ [Success] 06.10.2004 16:24:16 MUELLERC	16	BI AS Berechtigun	Authorization Gen	GENERATE	SEU_INT	CL_RSO_APIDialog pr	

At the bottom, a message box displays the following error:

Message Text
[Error] Hierarchy 0VCA_NC1_HIER_AUTH_22 (version , key date 31.12.9999) does not exist



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing and Test Tools

Migration

Summary

Pick one of these options to assign authorizations to users:

Management of Analysis Authorizations (RSECADMIN):

- 1. Assign Individual Authorizations**
- 2. Assign Groups of Authorizations**

Role Maintenance (PFCG):

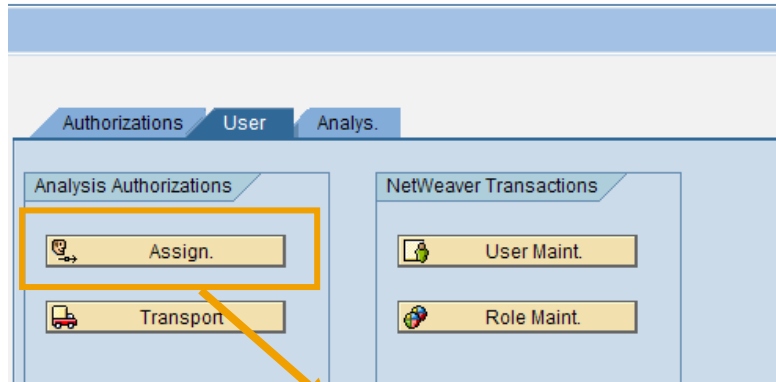
- 3. Assign Authorizations to Roles**

Tip: You can use a combination of these options. If you already have a role-based infrastructure in place, option 3 will be the best.

1. Assigning Individual Authorizations

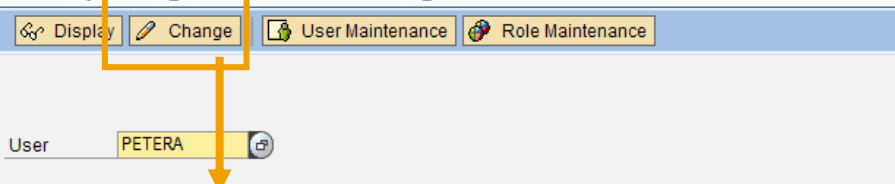
Direct Assignment of Authorizations to Users

Management of Analysis Authorizations

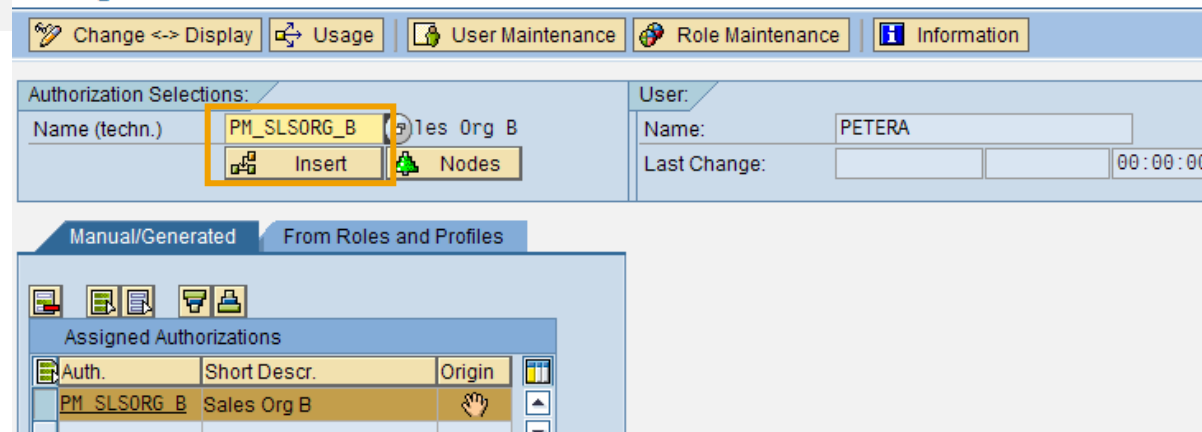


- Select a user ID and change the assignment
- Then insert individual authorizations to the assigned list

BI Reporting: Init Screen Assignment of User Authorizations



Assignment of User Authorizations: Edit



2. Assigning Groups of Authorizations

Assignment of Groups of Authorizations to Users

Assignment of User Authorizations: Edit

Change <-> Display Usage User Maintenance Role Maintenance Information

Authorization Selections: Name (techn.) PM_SLSORG_B Yes Org B

User: Name: PETERA Last Change: 00:00:00

Manual/Generated From Roles and Profiles

Assigned Authorizations

Auth.	Short Descr.	Origin
PM_SLSORG_B	Sales Org B	

Select hierarchy nodes

Hierarchy

- All hierarchies
 - Subset2
 - Subset1
 - AUTH10
 - AUTH11
 - AUTH12
 - AUTH13
 - Not Assigned Authorization (Tech) (s)

Continue Cancel

You can group authorizations into a hierarchy. Use InfoObject 0TCTAUTH for this hierarchy (you'll have to activate the content objects for this InfoObject).

Then you can assign one or several authorization groups to the selected user

Generated Special Authorization: OBI_ALL

- Automatically generated and not changeable
- Grants authorizations for all values of all authorization-relevant characteristics
- Adjusted whenever a new InfoObject is set to authorization-relevant
- Simple possibility to grant authorizations to everything (e.g., via role – see next slide)

Assignment of User Authorizations: Edit

Change <-> Display Usage User Maintenance Role Maintenance Information

Authorization Selections: Name (techn.) Insert Nodes

User: Name: PETERA Last Change: :00:00:00

Manual/Generated From Roles and Profiles

Assigned Authorizations

Auth	Short Descr.	Origin
OBI_ALL		
AUTH1		
AUTH10		
AUTH11		
AUTH12		
AUTH13		
AUTH14		
AUTH15		
AUTH16		
AUTH17		
AUTH18		
AUTH19		
AUTH2		
AUTH20		
AUTH21		
AUTH22		

3. Assigning Authorizations to Roles

Role Maintenance

- Alternatively to the direct assignment, you can also assign authorizations to roles, which can then be assigned to users
- Use authorization object S_RS_AUTH for the assignment of authorizations to roles
- Maintain the authorizations as values for field BIAUTH

Management of Analysis Authorizations

Change role: Authorizations

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Changed

PM_AUTH_ROLE Authorization role

- Manually Business Information Warehouse
 - Manually BI Analysis Authorizations in Role
 - Manually BI Analysis Authorizations in Role
 - BI Analysis Authorizations: Na *

Field values

Object S_RS_AUTH BI Analysis Authorizations in Role

Field Name BIAUTH BI Analysis Authorizations: Name of an Authoriz

Full authorization

From	To
PM_SLSORG_B	



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary

Use these tools for monitoring, auditing, and testing authorizations:

1. Authorization Monitoring
2. Legal Audit

Tip: The improved monitoring capabilities are especially helpful for production support

1. Authorization Monitoring

Checking Authorizations

- Log on with your own user ID (production support role)
- Check query execution with the authorizations of a specific user

The screenshot displays the SAP 'Management of Analysis Authorizations' interface. On the left, under 'Analysis Tools', the 'Execution as...' button is highlighted with an orange box and an arrow pointing to the right. The right-hand side shows the 'Execute as User with Restricted Authorizations' dialog. It features a text field for 'Execution as User:' containing 'JOHNPE'. Below this, a list of 'Possible Transactions' includes 'RSRT' (selected with a radio button), 'Reporting Agent Monitor', 'SEM Transaction UPSPL', 'SEM Transaction BPS0', 'MDX Test', and 'RSDRI Debug Program'. The 'With Log' checkbox is checked and enclosed in a dashed box. At the bottom, there is a 'Start Transaction' button with a green play icon.

Tip: There is no password required. Therefore, access to this support tool should be restricted using authorization object S_RSEC.

1. Authorization Monitoring (cont.)

Evaluate Log Protocol

- Turn on logging of user activities related to analysis authorizations
- View detailed information about authorization checks
 - ◆ Which characteristics are relevant?
 - ◆ Which selections are checked vs. which authorizations?
 - ◆ And much more ...

Management of Analysis Authorizations

Analysis Tools

- Execution as...
- Error Logs**
- Generation Logs

Log Management Analysis Authorizations

Information

Log for User: PETERA, Gener.: 14.07.2005 15:34:42

Display Delete Delete All

Add User Delete User

User That Is Being Logged

User	Alias
PETERA	

Display Error Log

Print Document Save Document

Authorization Check Log

Ausgeführt durch Benutzer **JOHNP**
Ausgeführt mit Analyseberechtigungen eines anderen Benutzers **URSEC04**
Ausgeführte Query: **FABAUTH8/PJADMIN02**

InfoProvider-Prüfung

Aufbau des Puffers...

Buffer Built

Gibt es Berechtigungen für den Zugriff auf folgenden InfoProvider? FABAUTH8
Berechtigung für allgemeinen Zugriff auf InfoProvider vorhanden FABAUTH8
Zugriffsaktivität: 03 ✓

Relevante Merkmale für die detaillierte Berechtigungsprüfung

(Merkmale mit voller Berechtigung werden nicht aufgelistet!)

Determining the Authorization-Relevant Characteristics:

List of Effective Authorization-Relevant Characteristics

OCOUNTRY

OFISCYEAR

(notenberechtigungen)

TRY




fragekombination berechtigt:

TLEVEL

2. Legal Auditing

Recording of Changes

- **Activate the following VirtualProviders from the Business Content (VAL = Values, HIE = Hierarchies, UA = User Assignment)**

ID	Object Name	Long Description
	OTCA_HIE	Change Document Analysis Authorization
	OTCA_UA	Change Document Authorizations
	OTCA_VAL	Change Document Analysis Authorization

- **The system records all changes to authorizations and user assignments**
- **Using a query, you can easily answer questions like:**
 - ◆ How many users have access to a given InfoCube?
 - ◆ Which users have access to company code 1000?
 - ◆ When was authorization GIVEMEALL created, and by whom?

2. Legal Auditing (cont.)

Recording of Changes

■ Query Example

Save View Bookmark Variable Screen Exceptions and Conditions Comments Export to Excel Export to CSV						
▼ Rows						
Authorization (Tech)						
Date						
InfoObject						
Last Changed By						
▼ Columns						
Key Figures						
▼ Free Characteristics						
+/- sign						
BW System						
Change Type Auth.						
Lower Value						
Object Version						
Selections Operator						
Time						
UTC Time Stamp						
Upper value						
Date	02.07.2005	Authorization (Tech)	RSR_00007060	InfoObject	Last Changed By	Number of Authorization Records
				BR9/A/0VCA_NC1	BR9/JOHNPE	2
				Result		2
				BR9/A/0VCA_NC1__0VCA_NC2	BR9/JOHNPE	6
				Result		6
				BR9/A/0VCA_NC2	BR9/JOHNPE	6
				Result		6
				BR9/A/0VCA_NC2R	BR9/JOHNPE	2
				Result		2
				Result		16
				RSR_00007071	BR9/JOHNPE	1
				Result		1
				BR9/A/0VCA_C1	BR9/JOHNPE	1
				Result		1
				Result		2
				Result		18
Date	03.07.2005	Authorization (Tech)	0BI_ALL	InfoObject	Last Changed By	Number of Authorization Records
				BR9/A/0APO_LOCNO	BR9/ULKE	1
				Result		1
				BR9/A/0CALYEAR	BR9/ULKE	1
				Result		1
				BR9/A/0COSTCENTER	BR9/ULKE	1
				Result		1
				BR9/A/0COUNTRY	BR9/ULKE	1
				Result		1
				BR9/A/0D_CUSTOMER	BR9/ULKE	1
				Result		1

■ Linked into Administration Cockpit



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary

Follow these four steps to migrate authorizations:

Migration Tool (program RSEC_MIGRATION):

- 1. Select Users**
- 2. Select Authorizations**
- 3. Pick Assignment Method**
- 4. Set Migration Mode**

Tip: Allocate enough time to do the migration during your system upgrade and for performing thorough tests

Migration Support

- **The migration is a singular event (i.e., not to be scheduled later)**
- **During migration to the new authorization concept, the existing concept won't be changed**
- **Semi-automatic migration**
 - ◆ **The more complex the existing authorization concept, the more manual migration work might be necessary**
 - ◆ **Customer-exit variables for 0TCTAUTHH cannot be migrated; the respective hierarchy nodes must be assigned manually**
 - ◆ **Intensive tests are highly recommended**

Before You Start (cont.)

Recommendations

- It is **highly recommended to migrate to the new concept**
- The former authorization concept won't be supported any longer
- You can, however, switch back to the former concept – in some exceptional cases (IMG setting)

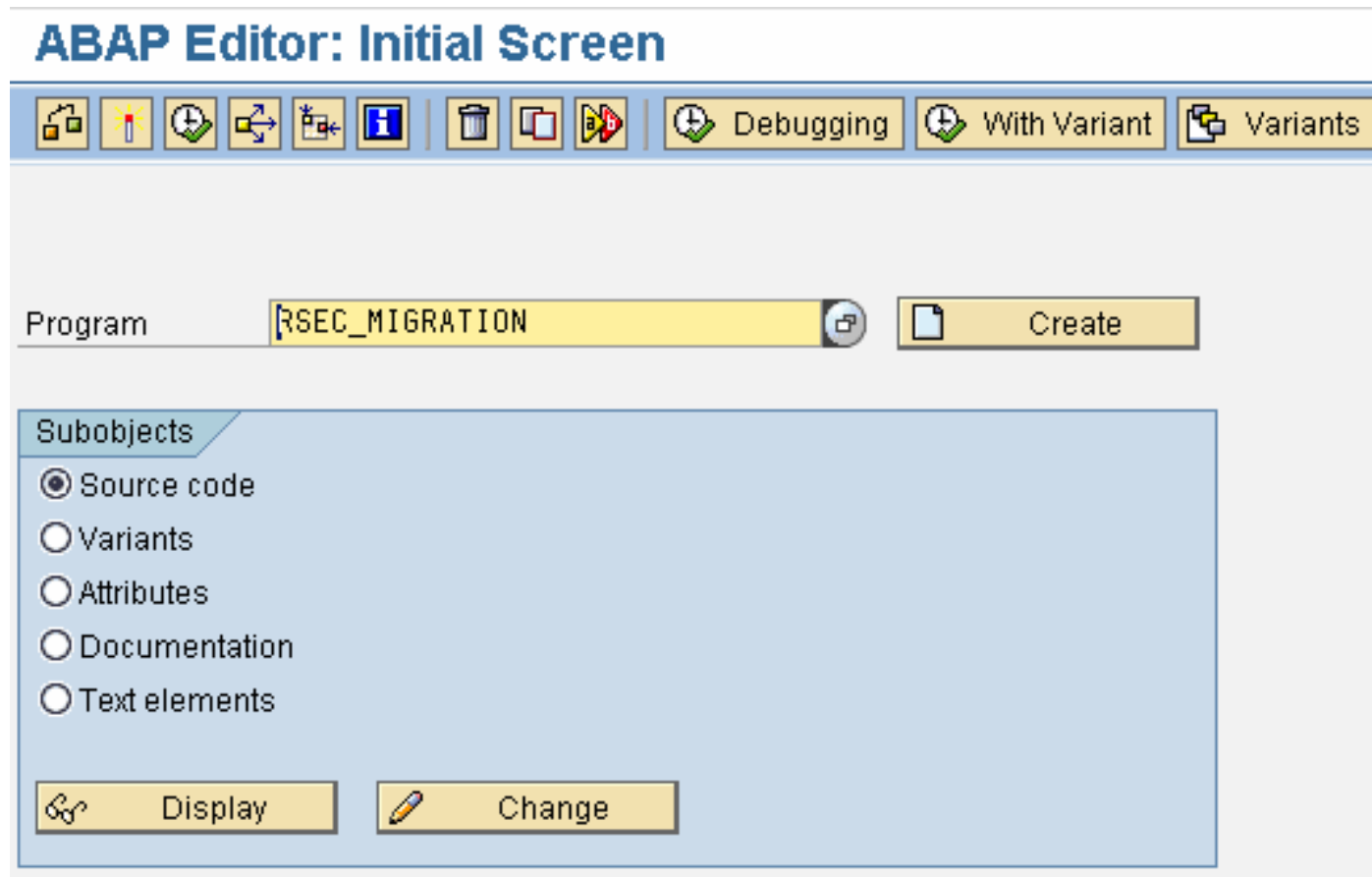
The screenshot displays the SAP IMG (Implementation Guide) interface. On the left, the 'Structure' pane shows the navigation path: SAP Customizing Implementation Guide > Activation Switch for SAP Enterprise Extension Set > SAP NetWeaver > SAP Business Information Warehouse > Reporting-relevant Settings > General Reporting Settings > Analysis Authorizations: Select Concept. An orange arrow points from this menu item to the right-hand pane.

The right-hand pane is titled 'Change View "Analysis Authorization System": Details'. It shows the 'Customizing ID' as 'Business Information Warehouse'. Under the 'Analysis Authorization System' section, the 'Authorization mode' dropdown menu is open, showing three options: 'Current Procedure with Analysis Authorizations' (highlighted in yellow), 'Obsolete Concept with RSR Authorization Objects', and 'Current Procedure with Analysis Authorizations' (highlighted in orange).

Start the Migration

Migration Step 0

- Run ABAP program RSEC_MIGRATION (transaction SA38 or SE38)

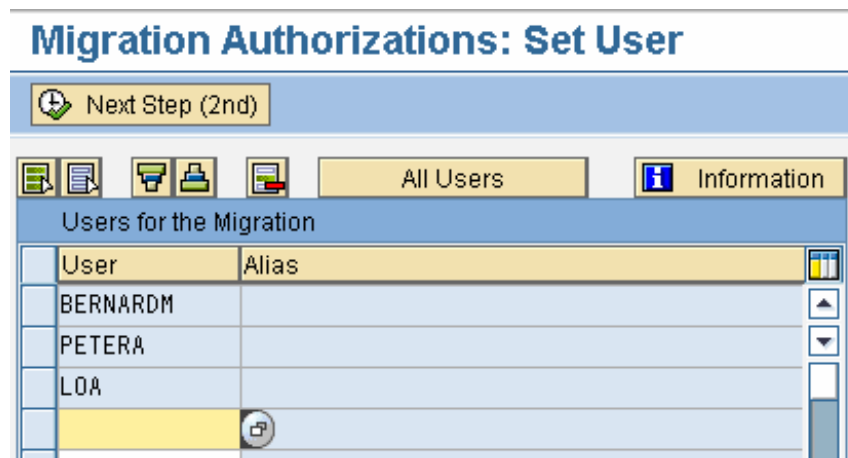


1. User Selection

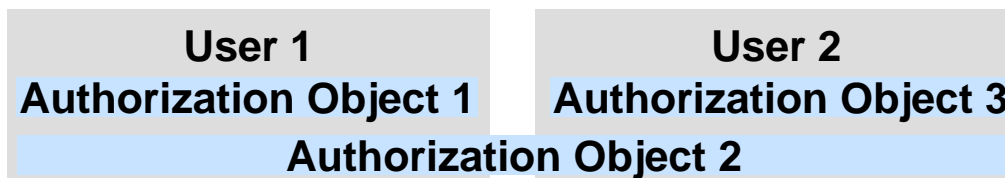
Migration Step 1

Choose users

- ◆ Migration can be done for singular user groups



- ◆ Prerequisite: A user group must be complete and self-contained!



Note: There might be entangled dependencies of users with respect to the authorization objects. You'll get a message with information on the missing users in case the user group is not complete.

If User 1 is chosen and Authorization Objects 1 and 2 should be migrated, you have to choose User 2 as well in order to have a complete user group

2. Authorization Selection

Migration Step 2

- Choose authorization objects to be migrated

Migration Authorizations: Authorization Objects

Next Step (3rd)

Reporting Authorization Objs. for Migration

Migrate	Authorization Object
<input type="checkbox"/>	YAUTHGEN
<input checked="" type="checkbox"/>	YRAC1
<input type="checkbox"/>	YRAD1
<input checked="" type="checkbox"/>	YRAH1
<input checked="" type="checkbox"/>	YRAM1
<input checked="" type="checkbox"/>	YRAN01
<input type="checkbox"/>	Z00HIER
<input checked="" type="checkbox"/>	ZDIV00
<input type="checkbox"/>	ZMB_AUTH
<input checked="" type="checkbox"/>	ZTR_AUTHPF
<input checked="" type="checkbox"/>	ZTR_COMP
<input type="checkbox"/>	S_RS_ICUBE
<input type="checkbox"/>	S_RS_ODSO
<input type="checkbox"/>	S_RS_ISET
<input type="checkbox"/>	S_RS_MPRO

3. Assignment Method

Migration Step 3

■ Choose an assignment method

◆ Direct user assignment

- Migrated authorizations will be assigned to the users directly (not via roles)
- Migrated authorizations have prefix RSR_ and will be treated like generated authorizations

◆ Create new profiles

- Generation of profiles based on authorization object S_RS_AUTH that contains the new, migrated authorizations
- Preserves the existing role concept and adds new profiles to the role
- Generated profiles have prefix RSR_

◆ Extend existing profiles

- Existing profiles will be extended by authorization object S_RS_AUTH containing the migrated authorizations

◆ Undo migration

- All migrated authorizations and profiles will be deleted; extended profiles contain empty authorization object R_RS_AUTH

The screenshot shows the 'Migration Authorizations: Characteristics' dialog box. At the top, there is a blue header bar with the title 'Migration Authorizations: Characteristics'. Below the header, there is a yellow button with a green arrow icon and the text 'Next Step (4th)'. The main area of the dialog is titled 'Select Assignment Method' and contains four radio button options: 'Direct Assignment to Users' (which is selected), 'Generate New Profile', 'Enhance Existing Profile', and 'Undo Migration'. To the right of each radio button is a blue information icon (a lowercase 'i' in a square).

4. Migration Mode


Migration Step 4

- **Choose details of authorization migration “expert mode”**
 - ◆ **Settings for referencing navigational attributes and characteristics are only relevant for the compatibility mode setting in SAP BW 3.x**
 - ◆ **Please have a look at the detailed documentation for more information**


Details of Migration: Characteristics


Execute Directly Execute in Background

Which Characteristics Receive Copies of Authoriz.?


 Explanations


Create Value Authorizations for


 Navigation Attributes (A..B)

 Referencing Navigation Attributes (A..BR)

Create Hierarchy Authorizations for

 Navigation Attributes (A...B)

 Referencing Navigation Attributes (A..BR)

 Referencing Characteristic (BRH)

After the Migration Run

Migration Protocol

- At the end of the migration run, view the detailed protocol
- Check for warnings and errors reported during the migration

Tip: The migration can be quite tricky. It helps if you have good documentation of the existing authorization setup (for example, to define user groups for the migration)

The screenshot shows the 'Protokolle anzeigen' window in SAP. The main table displays the migration log with columns for 'Datum/Uhrzeit/User', 'Anzahl', 'Externe Identifik...', 'Objekttext', 'Unterojekttext', 'Transakti...', 'Programm', and 'Mod...'. The log shows a successful migration run on 20.05.2005 at 13:30:43 by user JOHNPE, with a total of 44 messages. The messages include compatibility checks, user migration, reading of authorization data, deletion of old migration information, and construction of new authorizations. A detailed view of the messages is shown in the bottom pane.

Datum/Uhrzeit/User	Anzahl	Externe Identifik...	Objekttext	Unterojekttext	Transakti...	Programm	Mod...
20.05.2005 13:30:43 JOHNPE	44		Migration BI-Analy Generierung Bere Migration BI-Analy SE38			CL_RSO_APIDialog...	
[Detailed list of 44 messages follows, including compatibility checks, user migration, and authorization construction]							
20.05.2005 13:30:12 JOHNPE	6		Migration BI-Analy Generierung Bere Migration BI-Analy SE38			CL_RSO_APIDialog...	
20.05.2005 11:05:43 JOHNPE	6		Migration BI-Analy Generierung Bere Migration BI-Analy SEU_INT			CL_RSO_APIDialog...	



Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary

Where to Find Free Public Technical Information

SAP Developer Network (it's free and public)

SDN - The SAP Developer Network - Microsoft Internet Explorer provided by SAP IT

SAP DEVELOPER NETWORK

Welcome Lehment, Kristian

Home | Forums | Weblogs | Downloads | Services | Events | Pilot

Search

Go

SDN Content

Advanced search ...

Developer Areas

- SAP NetWeaver Platform
 - .NET Interoperability
 - Security**
 - Enterprise Portal
 - Knowledge Management
 - Business Information Warehouse
 - Exchange Infrastructure
 - Web Application Server
 - Mobile Infrastructure
 - Master Data Management
 - SAP xApps
 - Business One
 - Technologies

SAP NetWeaver™ Security

Enabling Single Sign-On from SAP J2EE Engine/EP to Non-SAP Java Applications

14 Sep 2004

Single Sign-On (SSO) is the standard secure authentication mechanism for Web-based applications in an SAP NetWeaver™ landscape. This article focuses on how to extend SSO to a Java-based web application NOT running on the SAP J2EE Engine. Follow this step-by-step example to create a servlet that receives an SAP logon cookie, validates it, and extracts the name of the user. The Attachments section contains the source code and a WAR file ready for deployment.

The Difference Between Logging and Tracing

20 Sep 2004

Logging, tracing...same thing, right? Nay! Behold the differences! This series of articles - about application instrumentation, monitoring, and management - aims to clarify those differences and identify patterns to make the distinctions clear. This article examines some of the most common scenarios and problems developers experience when they program a new application.

"Kosher" Hacking and How to Stop It

07 Sep 2004

Firewalls are not enough. 75% of all hacks today are executed in the application layer as opposed to the firewall-protected machine layer. The resulting financial losses are in the double-digit millions. Find out about two of the most popular hacking techniques--SQL Statement Injection and Cross-Site Scripting--and an application firewall as a means of prevention.

SAP Security Newsletter - August Edition

07 Sep 2004

This month's issue features an interview with SAP Chief Security Officer Dr. Sachar Paulus (PDF 37 KB).

Book Review: Security Engineering - A Guide to Building Dependable Distributed Systems

07 Sep 2004

Security knowledge is becoming increasingly important, even for those who don't have much time to devote to the subject. To help you on your way, SAP's security product management will provide a series of resource reviews so you can invest time wisely.

Single Sign-On in a Complex System Landscape

07 Sep 2004

Setting up Single Sign-On (SSO) between two components is relatively straightforward, but how do you go about setting up SSO in a large system landscape with many types of systems? This article provides an overview of the documentation from various areas and provides guidelines on how to set up SSO across several systems. It takes a look at a typical scenario, guiding you through the process of setting up SSO with SAP logon tickets. (PDF 266 KB)

Popular Documents

Updated 07 Sep 2004

- [Adding Security to Your J2EE Applications](#) (PDF 553 KB)
- [Security Patterns - Just another Way to Share Best Practices](#)
- [Migration to the SAP NetWeaver Architecture from a Security](#)

Featured Weblog

Quick Guide for Setting Up SSO between EP and R/3

Quick Links

- For a complete security overview see our [Security Solution Map](#)
- [Secure Store and Forward Developers' Guide](#)
- [service.sap.com/security](#)
- [service.sap.com/securitypartners](#)
- [service.sap.com/securityguide](#)
- [SAP NetWeaver Developers' Guide](#)

eLearning

- [Security eLearning](#)

Help

- [Security Documentation](#)

Local intranet

sdn.sap.com

Where to Find Application and Educational Information

SAP Service Marketplace/security

The screenshot displays the SAP Service Marketplace website in a Microsoft Internet Explorer browser. The address bar shows the URL <http://service.sap.com/security>. The page title is "SAP Service Marketplace" and the user is logged in as "Kristian Lehment". The main navigation menu includes "HOME", "myPage", "Solution Details", "Consulting", "Education", "Support", "Media Library", and "Communities". The "Security" section is active, showing a breadcrumb trail: "You are here: Security". The main content area features the heading "Secure Business with SAP" and the sub-heading "Without Security, Business Simply Cannot Prosper". Below this, there is a paragraph of text and a "News" section with several bullet points. A "Spotlight" section is also visible, featuring a link to the "Interactive SAP Security Solution Map".

Welcome, Kristian Lehment my Profile **SAP Service Marketplace** Other Portals | Quick Links | Help

SAP Service Channel - my Inbox Search Go! [Advanced Search](#)

HOME myPage Solution Details Consulting Education Support Media Library Communities

You are here: **Security** Feedback | Add to Favorites

Secure Business with SAP

Without Security, Business Simply Cannot Prosper

Data security at transaction level is a prerequisite to competing in the Internet economy. SAP offers best-in-class, comprehensive security solutions that protect data and ensure the confidentiality of business transactions. As a global solution provider and trusted advisor, SAP provides security technologies to protect the data processed by the mySAP Business Suite. The security infrastructure of SAP NetWeaver delivers comprehensive security features for heterogeneous environments. Combined with specialized partner solutions, its state-of-the-art technology makes mySAP Business Suite the secure place to do business. For information on specific security-related topics, see [Security in Detail](#)

News

- **Tutorial: How to create your own Java Custom Login Module** (August 2004)
If you need to secure an application you develop, you can do this using your own login module. This login module allows you to perform authentication in a different way to those provided with the J2EE Engine. By the end of this tutorial, you will be able to:
 - Use the SAP NetWeaver Developer Studio to develop your own login module.
 - Deploy the login module to the J2EE Engine.
 - Configure the login module on the J2EE Engine.
- **The SAP Security Newsletter for September 2004 is now available**
- **NetWeaver Security Guide Now Available** (April 2004)
Hot off the press, you can find the new SAP NetWeaver Security Guide in the [SAP Help Portal](#), or in the [SAP Service Marketplace](#). The guide provides an introduction to security with the SAP NetWeaver platform as well as individual security guides for each of the SAP NetWeaver components.
- **New SAP Security Certification for Consultants** (March 15, 2004)
SAP now offers a specialist security certification for consultants. Available to anyone with a background in technical consulting, security certification provides proof to customers of a consultant's knowledge in this area, as well as his or her ability to apply this knowledge practically in projects. You can find more information soon at [SAP Consultant Certification](#). Use the booking code C_TADMSEC_04 to register for certification. **You can also find previous issues of the SAP Security Newsletter in the [security newsletter archive](#).**

Spotlight

- The **SAP Security Solution Map** takes an outside-in approach, showing all the security aspects that companies require from their software. Under the individual topics, you can see whether SAP provides specific functionality or relies on partner products. You can take a look at the interactive map [here](#), or download the print version.
 - [Interactive SAP Security Solution Map](#)
 - [Print version SAP Security Solution Map](#) (PDF, 2649 KB)

Quick Link Information

Access this topic directly at <http://service.sap.com/netweaver>

Local intranet

service.sap.com



<http://sdn.sap.com>*

<http://service.sap.com/security>*

<http://service.sap.com/securityguide>*

<http://service.sap.com/education>*

<http://help.sap.com/nw2004s>

<mailto:security@sap.com>

*** Requires login credentials to the SAP Service Marketplace**

The central hub for the SAP technology community

- Everyone can connect, contribute and collaborate- consultants, administrators and developers
- Focus around SAP NetWeaver and SAP xApps

High quality of technical resources

- Articles, how-to guides, weblogs, collaborative areas, discussion forums and downloads, toolkits and code-samples

A collaboration platform, not a one-way street

- SAP experts from customers, partners and SAP

SDN is powered by SAP NetWeaver™

- Built on the SAP Enterprise Portal
- Featuring collaboration capabilities of SAP Knowledge Management

The screenshot shows the SAP Developer Network (SDN) website. At the top left is the SAP logo. The main header reads "SAP DEVELOPER NETWORK" and "Welcome Laurie Nolan". A navigation bar includes links for Home, Forums, Weblogs, Downloads, Services, Events, Pilot, DKOM 04, and My Rooms. Below the navigation is a search box with a "Go" button and a dropdown menu for "SDN Content". To the right of the search box is a section titled "Inside SDN" featuring a 3D wireframe cube icon and a link to "Save Time and Effort Analyzing Memory Problems in ABAP Programs with ABAP Memory Inspector". Below this link is the date "10 Feb 2005" and a short paragraph of text. On the left side of the page, there is a "Developer Areas" section with a list of categories: SAP NetWeaver Platform, Enterprise Portal, Knowledge Management, Business Information Warehouse, Exchange Infrastructure, Web Application Server, Mobile Infrastructure, Master Data Management, SAP xApps, Business One, and Technologies.

7 Key Points to Take Home

- **BI authorizations for analysis are based on an appropriate concept for business-oriented security requirements**
- **Using the new concept for analysis authorizations is recommended**
- **The new features contain major improvements for administrators, leading to lower TCO**
- **Authorizations can be generated automatically based on various DataStores**
- **The infrastructure for maintenance and monitoring of analysis authorizations is highly integrated**
- **Take a good look at the new reporting capabilities to support usage and auditing of authorizations**
- **A migration support tool is available**

Questions?



Q&A

marc.bernard@sap.com

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

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

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

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

Oracle is a registered trademark of Oracle Corporation.

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

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

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

Java is a registered trademark of Sun Microsystems, Inc.

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

MaxDB is a trademark of MySQL AB, Sweden.

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

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.

This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice.

SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.

The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.

