Strategic Enterprise Management: Security Guide

ADDON.SECGUIDE_SEM

Release 600

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

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

Typographic Conventions

Type Style	Description
Example text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.
	Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Strategic Enterprise Management: Security Guide

The following guide covers the information that you require to operate Strategic Enterprise Management (SEM) securely.

Introduction

Target Audience

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

The Need for Security

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system must not result in loss of information or processing time. These demands on security also apply to SAP Strategic Enterprise Management (SAP SEM). This Security Guide is intended to aid you in securing SAP SEM.

The security requirements of the various components of SAP SEM differ greatly from each other. These differences are described in detail below (where necessary):

- SAP SEM is positioned as a decision-making solution for corporate management. As a result, SEM normally processes only highly-aggregated data that rarely reveals sensitive details. (For example, it does not contain individualized personnel data.)
- However, the processes of analytical applications often have highly strategic significance for an enterprise and, therefore, require strict secrecy.
- In group consolidation, however, secrecy plays a small role since the intention is to meet the statutory disclosure requirements for publicly-listed enterprises; but, on the other hand, the complexity of the processes for meeting these disclosure requirements encourages the use of highly restrictive authorizations for accessing the system.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP SEM.

Overview of the Main Sections

The Security Guide has the following main sections:

- **Before You Start**

  This section contains information about why security is necessary, how to use this document, and contains references to other Security Guides that build the foundation for this Security Guide.

- **Technical System Landscape**

  This section provides an overview of the technical components and communication paths used by SAP SEM.

- **User Management and Authentication**

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

  - Recommended tools to use for user management
  - User types required for SAP SEM
  - Overview of the user synchronization strategy if several components or products are integrated

- **Authorizations**

  This section provides an overview of the authorization concept that applies to SAP SEM. It contains subsections with information regarding the SAP SEM components SEM-BCS, SEM-BPS, SEM-CPM, und SEM-SRM.

- **Network and Communication Security**

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

- **Data Storage Security**

  This section provides an overview of any critical data that is used by SAP SEM and the security mechanisms that apply.

Before You Start

Security Guides Referenced

SAP Strategic Enterprise Management (SAP SEM) is built on top of SAP NetWeaver Application Server ABAP. Therefore, the Security Guides of SAP NetWeaver also apply to SAP SEM. For a complete list of SAP Security Guides, see SAP Service Marketplace at **service.sap.com/securityguide**.

Additional Information

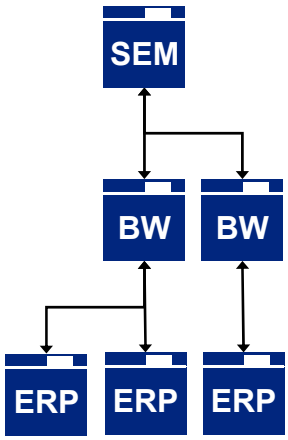
For more information about specific topics, see the links as shown in the table below.

Additional Information

Topic	SAP Service Marketplace
Security	service.sap.com/security
Security Guides	service.sap.com/securityguide
Related SAP Notes	service.sap.com/notes
Platforms permitted	service.sap.com/platforms
Network Security	service.sap.com/network service.sap.com/securityguide
SAP Solution Manager	service.sap.com/solutionmanager

Technical System Landscape

The following figure illustrates a typical system landscape for SAP Strategic Enterprise Management (SAP SEM):



SAP SEM works with data that is stored in SAP Business Information Warehouse (SAP BW). SAP SEM not only reads its data from SAP BW, but also modifies that data or creates new data and then writes the data back to SAP BW. The data in SAP BW is primarily fed from operational ERP systems. In the latter scenario, it is also possible to reverse the data flow by means of retractors [Extern].

The components shown in the figure can all reside on a single system or be distributed among several systems. In a landscape with distributed systems, data communication occurs using RFC [Extern] connections.

For more information about the technical system landscape, see the sources listed in the table below.

More Information About the Technical System Landscape

Topic	Guide/Tool	SAP Service Marketplace
Security		service.sap.com/security

User Management and Authentication

SAP SEM uses the user management and user authentication mechanisms of the SAP NetWeaver platform, in particular those of SAP NetWeaver Application Server ABAP. Consequently, the security recommendations and guidelines for user management and authentication described in SAP NetWeaver Application Server ABAP Security Guide [Extern] also apply to SAP SEM.

In addition to these guidelines, we provide you with information about user administration and authentication that specifically applies to SAP SEM in the following section:

- User Management [Seite 11]

  This section describes which user management tools to use, which user types are necessary, and which standard users are delivered with SAP SEM.

User Management

User management for SAP SEM uses the mechanisms provided by SAP NetWeaver Application Server for ABAP, such as tools, user types, and password policies. The following sections provide you with an overview of how these mechanisms affect SAP SEM. The standard users needed for operating SAP SEM are also listed.

User Management Tools

SAP SEM employs user and role maintenance of SAP NetWeaver AS ABAP (transactions SU01 and PFCG). For more information, see Users and Roles (BC-SEC-USR) [Extern].

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users that merely run processes in background jobs.

Examples of user types required for SAP SEM:

- Individual users:
  - Dialog users are employed for the configuration and live operation of all SEM components.
  - Internet users are employed for establishing connections to external websites that require logging in. A case in point is SEM Business Information Collection (SEM-BIC), which lets you configure automatic text searches in search engines or Internet databases.
- Technical users:
  - Communication users are employed for establishing RFC connections between the system running SAP SEM and the SAP BW system used as the data basis for SEM. The same applies to RFC connections between operational systems and SAP BW. These connections are essential for routine reporting of financial data from operational systems for group consolidations using SEM Business Consolidation (SEM-BCS).
    You also need these types of users to employ the transport tool provided in Financials Basis (FINBASIS). For example, SEM-BCS uses the transport tool to distribute Customizing data to live systems and clients.

For more information on these user types, see User Types [Extern] in the SAP NetWeaver AS ABAP Security Guide.

Authorizations

Use

SAP SEM uses the authorization concept provided in SAP NetWeaver. Consequently, the security recommendations and guidelines for user management described in the SAP NetWeaver AS ABAP Security Guide also apply to SAP SEM.

The SAP NetWeaver authorization concept allocates authorizations to users on the basis of roles. To define roles for ABAP technology, use the profile generator (transaction PFCG); to define roles for Java, use the user administration console of User Management Engine.

Standard Roles

This table lists the standard roles used in SAP SEM.

Standard Roles

Role	Description
SAP_BW_SEM_BCS_CORP_ACCOUNTANT	Corporate accountant
SAP_BW_SEM_BPS_APPLICATIONS	Reports of the planning applications in SEM
SAP_BW_SEM_LP	Liquidity planning
SAP_BW_SEM_RA_ALM_MANAGER	ALM manager
SAP_BW_SEM_RISK_CONTROLLER	SEM risk controller in SAP BW
SAP_BW_SEM_SRM_QUERIES	The information system SEM Stakeholder Relationship Management
SAP_SEM_ASSISTENT_TO_CFO	Assistant to the chief financial officer
SAP_SEM_BIC_ANALYST	Business Information Collection: Analysis
SAP_SEM_BIC_CUSTOMIZING	Business Information Collection: Basic settings
SAP_SEM_BPS_PLANNING	Business planning
SAP_SEM_CPM_BSC_PERS	SEM-CPM-BSC Web Application personalization role
SAP_SEM_CPM_BSC_REPORTING	Balanced Scorecard: Analysis
SAP_SEM_CPM_CUSTOMIZING	Corporate Performance Monitor: Basic settings
SAP_SEM_CPM_MC_REPORTING	Management Cockpit: Analysis
SAP_SEM_SRM	Stakeholder Relationship Management

Standard Authorization Objects

The following list shows references to documentation of the security-related authorization objects used by SAP SEM:

- Authorization objects in SEM Business Consolidation (SEM-BCS)
  - Authorizations for Master Data [Seite 14]
  - Authorizations for Tasks [Seite 18]

  SAP Note 651849 provides supplementary information over and above the two sections listed above.
- Authorization Objects in SEM Business Planning and Simulation (SEM-BPS) [Seite 23]
- Authorization Objects in SEM Corporate Performance Monitor (SEM-CPM) [Seite 26]

- Authorization Objects in SEM Stakeholder Relationship Management (SEM-SRM) [Seite 28]

Parallel Authorizations for Accessing Key Figures and Characteristics

When accessing characteristics and key figures, SAP SEM typically needs to consider the authorizations for InfoObjects defined in SAP Business Information Warehouse (SAP BW) in addition to the authorizations that are SEM-specific.

This makes it possible for you to define authorization profiles to allow or restrict access to characteristics and key figures in different ways. For example, you can use SEM-specific authorizations to grant the authorization for customizing the data model without permitting access to the key figure values contained in that data model. In contrast, a user for reporting requires dedicated authorizations for both SAP SEM and SAP BW. However, if a user has the reporting authorizations for SAP BW, but not for SAP SEM, that user will be able to execute BW queries but not be able to use the analysis features in SAP SEM.

Authorizations for Master Data

Use

You use this function to grant different privileges for accessing the characteristics of consolidation to persons who work with the SEM system.

Integration

The authorization concept of consolidation is embedded in the SAP authorization concept.

Features

Authorization checks can be made for all master data of consolidation.

For each characteristic you can determine how the authorization is to be assigned and checked:

- Per characteristic (for example, across all consolidation units) or
- Per characteristic value (for example, for each individual consolidation unit)

There are the following authorization objects:

- Authorization object **R_UGMD_CHA** is used for aggregate checking of characteristics in the local system.
- Authorization object **R_UGMD_SNG** is used for checking authorizations for individual characteristic values.
- Authorization object **S_TABU_LIN** (from SAP Basis) is also used for checking authorizations for individual characteristic values. This authorization object is still supported to ensure compatibility with Customizing you have made in earlier versions of SEM-BCS.

  The authorization objects **R_UGMD_SNG** and **S_TABU_LIN** are functionally the same. However, the use of generic authorization object **S_TABU_LIN** can result in some operational restrictions in certain situations (for example, no input help for characteristic values).

  We recommend that you use authorization object **R_UGMD_SNG** when checking authorizations for individual values. In Customizing you need to let the system know which of the authorization objects it should use.

In consolidation customizing, when you choose authorization checking for individual characteristic values of a characteristic, the system generates an organizational criterion when you use the authorization object **S_TABU_LIN**. The organizational criterion lets you make authorization assignments per characteristic value.

Master data can be stored in the SEM system and/or in the SAP Business Information Warehouse (SAP BW). A mechanism ensures that the master data of both systems is kept synchronized. In the same way, the authorization check is extended across all systems in which the characteristic resides. The BW system uses authorization object **S_RS_IOMAD**, which serves the same purpose as authorization object **R_UGMD_CHA** in the local system.

It is possible that you operate SAP BW and SEM in different physical systems. A user requires the same authorizations in all systems involved.

Activities

To assign authorizations for characteristics, you make the customizing settings listed below under the sections A to D:

A) Customizing Settings in the Consolidation Workbench

In the workbench you determine whether authorization checks are made per characteristic or per characteristic value.

1. In the process view of the workbench, choose *Data Model* → *Data Basis*.
2. Select the desired data basis using change mode.
3. Go to the *Authorizations* tab.

   The system displays all of the characteristics for which you can assign authorizations.
4. For each characteristic, determine whether authorization is to be checked per characteristic value.
5. Save the data basis.

   For those characteristics whose values are checked individually, the system generates an organizational criterion for each characteristic value when you use authorization object **S_TABU_LIN**. The organizational criterion lets you assign authorizations per characteristic value in role maintenance.

B) Customizing Settings in “Role Maintenance” (Transaction PFCG) in the Local System

1. In the local system, start role maintenance in the SAP menu by choosing *Tools* → *System Administration* → *User Maintenance* → *Role Administration* → *Roles*.
2. Specify an existing role or create a new role.
3. In role maintenance, go to the *Authorizations* tab and choose *Change Authorization Data*.
4. Go to authorization maintenance and activate the authorizations as follows:
   - Define the aggregate authorizations for the desired characteristics (authorization object **R_UGMD_CHA**) under *Strategic Enterprise Management* → *Master Data: Characteristics*.
   - Define the authorizations for individual characteristic values. Use one of the following authorization objects for this:
     - Authorization object **R_UGMD_SNG**: *Financials Basis* → *Characteristic Values: Master Data*
     - Authorization objects **S_TABU_LIN**: *Basis Administration* → *Authorization for Organizational Unit*.
5. Save the authorizations.

C) Customizing Settings in the BW System

C) 1. Customizing Settings in Characteristic Maintenance

1. In the BW System, activate authorization assignments per characteristic value as follows: Maintain the desired characteristic, go to the *Master Data/Texts* tab, and select the indicator *Master Data Maintenance with Authorization Check*.
2. Save the characteristic.

C) 2. Customizing Settings in "Role Maintenance" (Transaction PFCG)

Proceed the same way as for the authorization assignments in the local system – that is, define the following authorizations:

- The authorizations for individual characteristic values (authorization object **R_UGMD_SNG** or **S_TABU_LIN**)
- The aggregate authorizations for characteristics (authorization object **S_RS_IOMAD**)

D) Final Settings for Checking Characteristic Value Authorizations

If you have opted for an authorization assignment at the level of characteristic values, define which of the available authorization objects should be included in the authorization check:

1. Start transaction **UG01**.

   The *Display Area Menu UG01* screen appears.

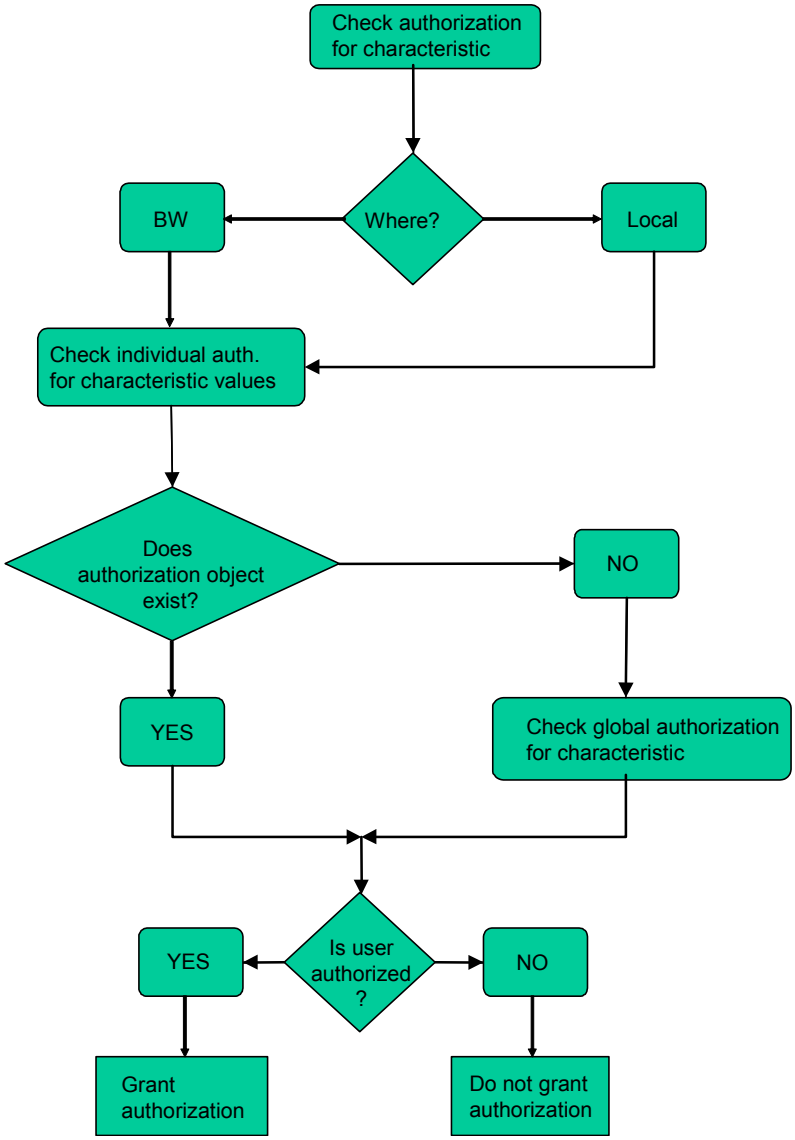
2. In the menu structure, choose *Master Data Settings* → *Parameter Settings*.
3. In the table, search for the parameter *Use Authorization Object R_UGMD_SNG for All Fields*. If no entry exists for this parameter yet, create a new entry and assign the parameters.
4. Decide which authorization object the system should use for checking authorizations for individual characteristic values:
   - To use authorization object **R_UGMD_SNG** enter **X** under *Parameter Value*.
   - To use authorization object **R_UGMD_SNG**, do not enter anything under *Parameter Value*.
5. Save the settings.

   If you do **not** perform the settings described above, the system assumes that the generic authorization object **S_TABU_LIN** is to be used for checking characteristic authorizations in order to ensure downward compatibility.

E) Authorization Checking (System Activity)

Once you have made the customizing settings, the system is able to perform authorization checks for characteristic as defined. The system uses the following procedure:



See also

SAP Authorization Concept [Extern]

Authorizations for Tasks

Use

You use this function to grant various privileges for accessing consolidation tasks to persons who work with the SEM System.

You want to grant the following authorizations to a group of users in consolidation area 01 in all versions:

- For data collection tasks and for consolidation groups A – C you grant the following authorizations:

a. Block

b. Unblock

c. Execute in test mode

d. Execute in update mode

e. Change task status

- For all other tasks and all other consolidation groups (D - H) you grant the following authorization:

  a) Execute task in test mode

To grant authorizations for the Customizing of tasks, follow the steps described in Authorizations for Master Data [Seite 14].

Integration

The authorization concept of consolidation is embedded in the SAP authorization concept.

Prerequisites

You have created at least one consolidation area [Extern] for which you want to customize the authorizations for tasks.

You have completed the Customizing settings for the tasks of consolidation. This means that:

- You have customized the individual tasks.
- You have set up the Task Hierarchy and Sequence [Extern] as well as the hierarchy of consolidation units to be able to execute the tasks in update mode.

Features

You can grant authorizations for:

- Executing tasks in both update mode and test mode
- Blocking and unblocking tasks
- Changing the status of tasks

The authorizations apply to each separate consolidation area.

You can restrict authorizations to the following, status-relevant characteristics:

- Specific versions
- Specific consolidation groups

- Specific consolidation units

The authorizations you grant for higher-level consolidation groups also apply to that group's lower-level consolidation groups and units.

You use authorization object **R_UC_TASK** to make the assignments. This authorization object has the following fields:

- *Activity,* which has the following attributes:
    f. *Block task*
    g. *Unblock task*
    h. *Execute task in update mode*
    i. *Execute task in test mode (simulation)*
    j. *Change status of task*
- Consolidation area
- Task

  All tasks within the consolidation area are available.
- *Fields 1 through 7*

  All characteristics with roles *version, consolidation group,* or *consolidation unit* are available.

  If more than seven fields exist for restricting an authorization (for example, if you have 4 characteristics for versions, 2 for consolidation groups, and two for consolidation units), then in Customizing of the consolidation area you should explicitly specify each and every characteristic you want to use for restricting the authorization. Then, these characteristics will be available automatically when you maintain the roles.

The consolidation monitor checks the authorizations of the user for the respective activities.

- If the user possesses the necessary authorization, the system carries out the activity.
- If the user does not possess the necessary authorization, the system does not carry out the activity and, instead, displays an error message.

Activities

To assign authorizations for tasks, you make the following Customizing settings:

A. Customizing of the consolidation area—*only if more than seven fields exist for version, consolidation group, and consolidation unit*

If you have more than seven fields for restricting task authorizations, proceed as follows:

1. Go to the process view of the workbench and choose *Data Model* → *Consolidation Area*.
2. Select the desired consolidation area using change mode.
3. On the *Fields* tab page, go to the column *Use Characteristic for Authorization Checks of Tasks* and select the indicator for those characteristics you want to use to restrict authorizations. (You can do this for up to seven characteristics.)
4. Save the consolidation area.

B. Customizing settings in "Role Maintenance" (transaction PFCG)

1. In the local system, start role maintenance in the SAP menu by choosing *Tools* → *System Administration* → *User Maintenance* → *Roles*.
2. Specify an existing role or create a new role.

3. In role maintenance, go to the *Authorizations* tab and choose *Authorization Data*.
4. Go to *Strategic Enterprise Management → SEM-BCS: Authorization Check for Task* and define the authorizations for the following:
   - Consolidation area (single value only)
   - Activity (or combination thereof; wildcard (*) possible)
   - Task (or multiple tasks; wildcard (*) possible)
   - If applicable, other characteristics for version, consolidation group, and consolidation unit (combination and wildcard (*) possible)

   See also the example below.

   Caution:

   Up to Release 3.1B, the space characters ( ) **and** asterisks (*) were used as wildcards for all values. Starting in Release 3.2, entering an asterisk (*) for the consolidation unit grants authorization to all existing consolidation units for posting levels 01 through 10.
5. Save the authorizations.
6. Generate the role.

C. Authorization checking (system activity)

Once you have completed the customizing settings, the system is able to perform authorization checks for the activities in the consolidation monitor according to your definitions.

Example 1

Let's use the example stated at the beginning of this topic.

You can achieve the authorization assignments by making the following Customizing settings: In Role Maintenance you specify the following parameters for the desired role (under *Strategic Enterprise Management → SEM-BCS: Authorization Check for Task*):

Manual: Authorization check for task

Activity	Block, unblock, simulate, execute in update mode, change task status
Consolidation area	01
Task	Collection of reported financial data; collection of additional financial data
1st Characteristic	Consolidation group A - C
2nd Characteristic	*
3rd Characteristic	*
4th Characteristic	*
5th Characteristic	*
6th Characteristic	*
7th Characteristic	*

Manual: Authorization check for task

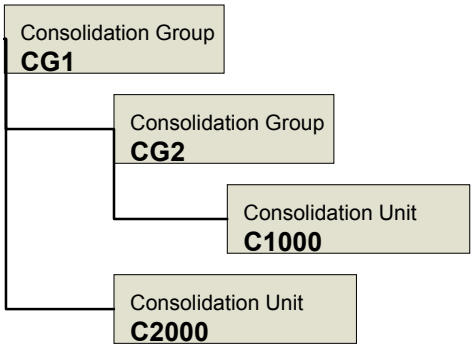
Activity	Execute in test mode
Consolidation area	01

Task	Balance carryforward, validation of reported financial data, standardization of reported financial data, reconciliation, currency translation and rounding, validation of standardized financial data, elimination of IU payables/receivables, elimination of IU profit/loss in inventory, consolidation of investments, reclassifications, allocation, validation of consolidated data
1st Characteristic	Consolidation group D - H
2nd Characteristic	*
3rd Characteristic	*
4th Characteristic	*
5th Characteristic	*
6th Characteristic	*
7th Characteristic	*

Example 2

The authorizations you grant for higher-level consolidation groups also apply to that group's lower-level consolidation groups and units.

Initial situation:



Settings affect the authorizations as follows:

Posting Level	Task	Cons Group	Cons Unit	Result
00-10	T1	CG2	<blank>	Authorization to execute task T1 for consolidation unit C1000
00-10	T1	CG1	<blank>	Authorization to execute task T1 for consolidation units C1000 and C2000
00-10	T1	CG2	C2000	Authorization to execute task T1 for consolidation units C1000 and C2000
02,12,20,22,30	T2	CG2	<blank>	Authorization to execute task T2 for consolidation group CG2
02,12,20,22,30	T2	CG1	<blank>	Authorization to execute task T2 for consolidation groups CG1 and CG2

See also

- Authorizations for Master Data [Seite 14]
- The SAP Authorization Concept [Extern]

Authorizations

Use

The activities that you can carry out in SAP SEM-BPS are covered by the SAP authorization concept. This means that you can assign different access rights to planning functionality to the people who work with the SEM System.

Integration

The system checks the special authorization objects that SEM-BPS defines and, if necessary, also those authorization objects that are defined for reporting in the SAP Business Information Warehouse environment. In this case, the SEM-BPS users must have both the SEM-BPS application-specific authorizations and the general SAP BW reporting authorizations. You manage the SEM-BPS authorizations using the system administration tools (see Users and Roles [Extern]) and the BW reporting authorizations using the relevant functions under *Business Explorer* → *Authorizations* → *Reporting - Authorization Objects*.

To assign authorizations for changing and displaying plan data separately, you must include the ACTVT (activity) field in the reporting authorization object. In this field the value 02 represents the authorization to change and 03 the authorization to display plan data. If you do not include the field, then this corresponds to an authorization to change plan data.

In addition to that, because of internal dependencies, you need authorization for the following authorization objects for data entry using planning layouts:

- **S_BDS_DS**: This authorization object controls access to documents, which belong to a document set of the Business Document Service (BDS).
- **S_TRANSLAT**: This authorization object controls access to the translation functions of the SAP System.

Features

The following authorization objects exist for the SEM Business Planning and Simulation component:

- **R_AREA**: You use this authorization object to control access to planning areas and all subordinate objects. You must set up read access to planning areas for people who will work with the SEM-BPS component. Otherwise, they will not be able to access any of the subordinate planning elements.
- **R_PLEVEL**: You use this authorization object to control access to planning levels and all subordinate objects. This authorization object is also relevant to access documents of the SEM-BIC component.
- **R_PACKAGE**: You use this authorization object to control access to planning packages (including ad hoc packages).
- **R_METHOD**: You use this authorization object to control access to planning functions and the appropriate parameter groups.
- **R_PARAM**: You use this authorization group to control access to individual parameter groups of a certain planning function.
- **R_BUNDLE**: You use this authorization object to control access to global planning sequences (you control authorizations for planning sequences, which you create for a planning level, with the authorization objects **R_METHOD**, **R_PLEVEL**, or **R_AREA**).

No separate authorization for execution is defined for this authorization object. Whether a global planning sequence can be executed or not, depends on the authorization objects for the planning functions contained in it.

- **R_PROFILE**: You use this authorization object to control access to planning profiles. A planning profile restricts the objects that can be viewed. If you wish to view the planning objects, you must have at least display authorization for the appropriate planning profile.
- **R_PM_NAME**: You use this authorization object to control access to planning folders. In order to be able to work with planning folders, you also require the necessary authorizations for the planning objects combined in the folder.
- **R_WEBITF**: You use this authorization object to control access to Web interfaces that you create and edit with the Web Interface Builder, and from which you can generate Web-enabled BSP applications.
- **R_STS_PT**: You use this authorization object to control access to the Status and Tracking System. The object enables a check to be carried out whether a user is allowed access to a certain subplan or a version of it with the Status and Tracking System.
- **R_STS_CUST**: You use this authorization object to control access to Customizing for the Status and Tracking System. The object enables or forbids a user to execute Customizing.
- **R_STS_SUP**: This authorization object provides the assigned users with the status of a superuser in relation to the Status and Tracking System. The object enables changing access to all plan data, independent of whether and where a user of the cost center hierarchy it is based on is assigned. The authorization object is intended for members of a staff controller group, who are not part of the line organization [Extern] of the company, but who nevertheless must be able to intervene in the planning process.

In accordance with the hierarchical relationships that exist between the various types of planning objects, authorizations that are assigned to an object on a higher level are passed on to its subordinate objects. An authorization that has been passed on can be enhanced but not restricted on a lower level. The following table presents the combination possibilities using the example of a change authorization for planning area and level:

Change Planning Area	Change Planning Level	Authorization Available for Level
yes	no	yes
yes	yes	yes
no	no	no
no	yes	yes

In practice this behavior means that you can proceed according to two different strategies when setting up authorizations:

- *Minimization of Customizing Effort*: You assign authorizations for planning objects on as high a level as possible, and thereby enable access to the planning objects without further authorization assignment on lower levels.
- *Optimization of Delimitation of Access Rights*: You assign authorizations for planning objects on as low a level as possible, and therefore make sure that access to a planning object is only possible for the person responsible for this.

Activities

Create the user profiles you require and then assign authorization objects to these profiles. Then assign the newly created user profiles to possible users.

You can find further information on the activities associated with the different authorization objects in the online documentation on the authorization objects themselves. You can call this up in the maintenance transaction "Role maintenance" (**PFCG**).

Authorizations

Use

The activities that you can perform in Strategy Management or Performance Measurement are all handled by the SAP authorization concept. This means that you can grant users working with Strategy Management or Performance Measurement different types of access to the available functions.

Integration

The system checks the special authorization objects defined in Strategy Management or Performance Measurement, as well as any existing authorization objects defined in the environment of the SAP Business Information Warehouse [Extern] (SAP BW) for reporting functions. In such cases, you therefore need to have the application-specific authorizations in Strategy Management or Performance Measurement as well as the general reporting authorizations in SAP BW. You manage the authorizations for BW reporting using the function designed for this purpose under *Business Explorer → Reporting Authorization Objects.*

Features

The authorization objects listed in this section exist for Strategy Management or Performance Measurement. For detailed information on these authorization objects, see the system documentation that you can call up during authorization object maintenance (transaction SU21).

- **R_COCKPIT**: You use this authorization object to control access to objects edited with the *Management Cockpit* function.
- **R_CPM_BSC**: You use this authorization object to control access to objects edited with the *Balanced Scorecard* function.

  The authorization object **R_SCARD** is now obsolete and is no longer used in authorization checks for the Balanced Scorecard.
- **R_MEAS**: You use this authorization object to control access to measures that you create and edit with the Measure Builder function. To be able to edit a measure, users need to have the authorization for editing objects on the corresponding hierarchy level of the measure catalog. This authorization is controlled using the authorization object **R_HIERNODE**.
- **R_HIERNODE**: You use this authorization object to control access to a specific hierarchy level of the measure catalog in the Measure Builder. Authorizations for editing measures can therefore be managed with this authorization object in combination with the authorization object **R_MEAS**.

  The authorization object **R_HIER** is now obsolete and is no longer used in authorization checks for the Measure Builder.
- **R_RMS**: You use this authorization object to control access in Risk Management to scorecards located in the target system that are involved in risk analysis.
- **R_RISK**: You use this authorization object to control access in Risk Management to individual risks that you have modeled.
- **R_RCNODE**: You use this authorization object to control access in Risk Management to hierarchy nodes in the risk catalog.

- **R_VDTREE**: You use this authorization object to control access to the design and display functions for the Value Driver Tree.
- **R_BSC_EBB**: You use this authorization object to control access to the Briefing Book Designer.

Note that the authorization objects relevant for SEM-CPM are divided into different authorization object classes:

Partial Application	Authorization Object Class
Measure Builder	MB
Balanced Scorecard, Management Cockpit, Risk Management, Value Driver Tree	SEM

To use the translation function in the Measure Builder, you also need the following standard authorization object:

- **S_TRANSLAT**: You use this authorization object to control access to the translation function in the measure catalog in the Measure Builder. Enter the following values into the fields of the authorization object:
  - **ACTVTY**: **02**
  - **TLANGUAGE**: Desired target language for the translation
  - **TRANOBJ**: **SHRT**

Activities

In the SEM menu, choose *Strategic Enterprise Management* → *Strategy Management* → *Design* → *Various* → *Authorizations* to define authorizations.

Create the user profiles you need and assign the desired authorization objects to these profiles. Then assign the new user profiles to the appropriate users.

See also:

Role Maintenance [Extern]

Authorizations

Use

The activities that you can carry out in SAP SEM-SRM are covered by the SAP authorization concept. This means that you can grant users working with the SEM System different levels of access to the Stakeholder Management functions.

Integration

The system checks the special authorization objects that SEM-SRM defines and, if necessary, also those authorization objects that are defined for reporting in the SAP Business Information Warehouse. In this case, the SEM-SRM users must have both the SEM-SRM application-specific authorizations and the general SAP BW reporting authorizations. You manage the SEM-SRM authorizations using the system administration tools (see Users and Roles [Extern]) and the BW reporting authorizations using the relevant functions under *Business Explorer → Authorizations → Reporting - Authorization Objects*.

Furthermore, you can set up highly differentiated authorizations using the SAP business partner tools for this purpose. You find the relevant functions in the IMG documentation by choosing *Cross-Application Components → SAP Business Partner → Basic Settings → Authorization Management*.

Included in the Customizing options for the SAP business partner is the option of changing for each customer the way the different fields and field groups are distributed across the tab pages for SEM-SRM Stakeholder Management. However, the authorization concept is set up so that fields not intended for unauthorized access remain protected in all cases – independently of where the field appears in SEM-SRM.

Features

The following authorization objects exist for the SEM Stakeholder Relationship Management component:

- **R_STHOLDER**: You use this authorization object to control access to stakeholders known in the system. Here, access applies to all information made available on a stakeholder (expectations, contacts, stocks owned, and so forth).

  The authorization object for accessing stakeholders also offers the option of specifying the stakeholder group(s) that an authorization is to be given to. This means that access is only made available to members belonging to certain groups, which saves you the effort of having to list group members individually and having to modify the authorizations once changes have occurred.

- **R_DOCUMENT**: You use this authorization object to control access to documents. Besides defining access authorization for individual documents, you can also differentiate authorizations according to the document group, which in terms of practicality is the more efficient application of authorization objects.

- **R_CONTACT**: You use this authorization object to control access to contacts stored for a stakeholder. Besides defining access authorizations for individual documents, you can also differentiate authorizations according to the contact type (such as mailing action, personal conversation, and so forth).

Activities

You create the user profiles you require and then assign authorization objects to these profiles. Then you assign the newly created user profiles to specific users.

You can find further information on the activities associated with the different authorization objects in the online documentation on the authorization objects themselves. You can call this up in the maintenance transaction "Role maintenance" (**PFCG**).

Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP SEM is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to SAP SEM.

Special Considerations for the System Landscape of SAP SEM

As described in Technical System Landscape [Seite 9], SAP SEM works almost exclusively with aggregated data, which is attained by first uploading data into SAP Business Information Warehouse (SAP BW) and then aggregating that data. For the functions of SAP SEM it is insignificant whether SAP SEM and SAP BW are operated on the same system or separate systems. However, from the communication security standpoint, which system landscape you decide upon has different consequences:

- If you opt for separate systems (for example, to assign entire user groups to different systems), you need to set up an individual RFC destination for each application in SAP SEM, which will be used to communicate between the SEM and BW systems. You need to secure these additional RFC destinations as you normally would.
- However, if you operate SAP SEM and SAP BW on the same system, there is no need to set up and secure these RFC destinations.

For more information, see the following sections in the SAP NetWeaver Security Guide:

- Network and Communication Security [Extern]
- Security Aspects for Connectivity and Interoperability [Extern]

Data Storage Security

SAP SEM uses SAP Business Information Warehouse (SAP BW) as its data basis. Thus, the authorizations that are most significant for the security of data are those for accessing the SAP BW system, in general, and those for accessing the InfoObjects contained in SAP BW, in particular.

Furthermore, some SAP SEM applications utilize local data buffers. This accelerates data access times by bypassing read accesses to SAP BW. SEM-CPM and SEM-SRM are applications that use this technique.

Locally-buffered data is always on the system that runs SAP SEM. If your security policy is based on the assumption that access to SAP BW is required to read the data, then the use of local data buffers may compromise this policy because, in this case, it is possible to access the buffered data without checking for authorizations that apply to SAP BW.

One possible solution for this problem may be to configure the SAP SEM applications so that no data buffering takes place and data is always read directly from SAP BW. Another solution may be to define SAP SEM-specific authorizations that are more restrictive to ensure that only staff with official authorization is granted access to data in the SEM system.