PUBLIC
2021-07-23

Security Guide for SAP Business Planning and Consolidation 10.1, version for SAP NetWeaver

THE BEST RUN SAP

Content

1 Document History

An overview of important changes made to this document since its initial release.

Date	Description
2014 June 24	Initial version.
2014 September 15	Updated the topic "Important SAP Notes" in Before You Start [page 8] for SP3.
2014 November 28	Updated the topic "Important SAP Notes" for SP4. Also, added the topic Authorization Objects for Modeling (Embedded only) [page 38].
2015 June 08	Added the section "Preventing Clickjacking in the Web Client" to the topic Other Security-Relevant Information [page 53].
2016 September 11	Added the section "Dynamic CSRF Token" to the topic Other Security-Relevant Information [page 53].
2016 July 21	In the section "General Rules for Data Access Security" in the topic Data Access Profile Setup (Standard only) [page 27], removed the bullet stating that denial of data access can be set only at the user level.
2016 August 29	In the section "Creating a Data Access Profile" in the topic Authorization Levels and Their Precedence (Embedded only) [page 43], added information to the note about how you can further define a selection range according to the relationship and level of a member you select in the hierarchy.
2016 October 18	Added the topic Authorization Objects for Performing Consolidation Tasks (Embedded only) [page 42].
2016 October 26	In the "Authorizations" chapter: • Added teams to the last step of the procedure in the "Creating Data Access Profiles" section of Data Access Profile Setup (Standard only) [page 27]. • Added teams to the last step of the procedure in the "Creating a Data Access Profile" section of Authorization Levels and Their Precedence (Embedded only) [page 43]. • Added the topic Integrating with Central User Authorization [page 34].

Date	Description
2016 November 21	In Authorization Objects for Performing Consolidation Tasks (Embedded only) [page 42], added field names and activities for the authorization object Manage Control.
2016 December 09	In Authorization Objects for Performing Consolidation Tasks (Embedded only) [page 42], added a note that installation of these authorization objects is not required if you do not intend to perform consolidation-related functions.
2017 April 20	• In the Introduction [page 19] to "Authorizations", added that you use data access profiles to define the models and data within those models to which users have access. • In Authorization Objects for SAP Business Explorer [page 35], added steps for maintaining the authorization objects for users. • In Authorization Objects for Administration (Embedded only) [page 36], added steps for maintaining the authorization objects for users. • The title of Authorization Objects for Modeling (Embedded only) [page 38] was changed from "Authorization for Maintaining Dimension Master Data" and added information about maintaining central and local master data, creating and maintaining local InfoProviders, and maintaining central and local hierarchies. • Added the topic Authorization Objects for Reporting and Planning (Embedded only) [page 40]
2017 June 19	Added the topic Authorization Objects for Maintaining Data Access Profile (Embedded only) [page 38].
2017 August 1	In Authorization Objects for Reporting and Planning (Embedded only) [page 40], added information to the section "Working with System Reports".
2017 November 16	Added the section Data Protection and Privacy [page 56].

2 Introduction

This document is not included as part of the Installation guides, Administrator's guides, or Upgrade guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security guides provide information that is relevant for all life cycle phases.

In the 10.1 release, two product variations called *embedded* and *standard* are supported based on the way your installation is configured. When information in this guide applies to only one of the configuration types, the title of the topic contains an indicator of either *(Embedded only)* or *(Standard only)*. A topic that contains no indicator in its title applies to both the embedded and standard configuration of the application. Also, information within a single topic that differs between the configuration types will be clearly explained within the relevant content.

> ⚠ Caution
>
> Planning and Consolidation does not store or display personal data, but does store or display items such as IP addresses and e-mail addresses. For example, log files can contain IP addresses and the database can contain e-mail addresses. You should bear this in mind before you distribute Planning and Consolidation log files or data to third parties.

Why is Security Necessary

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 on your system should not result in loss of information or processing time. These demands on security apply likewise to Planning and Consolidation. To assist you in securing your system, we provide this Security Guide.

Event and Notification (Standard only)

The event and notification function supports the creation of messages and their delivery as notifications or alerts in the application framework or as e-mails. Since messages can be sent to different users and groups and can contain hyperlinks to allow users to directly perform certain actions, security considerations might apply, which are specific to the scenario implemented by event and notification.

About This Document

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

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**
  This section contains references to other security guides that build the foundation for this security guide.
- **Technical System Landscape**
  This section contains a link to more information about the system landscape.
- **Security Overview**
  This section explains the initial users in the system and default authorizations. The section also provides an overview of the high-level steps needed to establish Planning and Consolidation security.
- **User Administration and Authentication**
  This section provides an overview of the following user administration and authentication aspects:
  - User management
  - Integration into single sign-on environments
  - User setup (standard only)
  - Team setup
- **Authorizations**
  This section provides details on the authorization concept that applies to Planning and Consolidation.
- **Network and Communication Security**
  This section provides an overview of the network topology and communication protocols used by the application.
- **Data Storage Security**
  This section describes the security aspects involved with saving data used by the application.
- **Other Security-Relevant Information**
  This section describes other security considerations.
- **Dispensable Functions with Impact on Security**
  This section describes which functions are not absolutely necessary and how you can deactivate them.

3 Before You Start

Fundamental Security Guides

The application is built with SAP NetWeaver components. The framework comprises an SAPUI5 client coupled with SAP NetWeaver server-side components. The SAP NetWeaver Security Guides also apply to the application. Pay particular attention to the *Most-Relevant Sections or Specific Restrictions* as indicated in the table.

Scenario, Application, or Component Security Guide	Most-Relevant Sections or Specific Restrictions
SAP NetWeaver Application Server ABAP Security Guide on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	AS ABAP Authorization Concept
Identity management information on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	User and Role Administration of AS ABAP
User authentication and single sign-on information on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	Authentication on the AS ABAP
RFC/ICF Security Guide on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	-
SAP NetWeaver Security Guide on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	Secure Network Communications (SNC)
SAP NetWeaver documentation on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	ABAP Programming and Runtime Environment (BC-ABA)
Security Guides for Connectivity and Interoperability Technologies on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	-
SAP NetWeaver documentation on SAP Help Portal at http://help.sap.com *SAP NetWeaver*	Network and Transport Layer Security

For a complete list of the available SAP Security Guides, see http://service.sap.com/securityguide on the SAP Service Marketplace.

Important SAP Notes

The most important SAP Notes that apply to the security of the system are shown in the table below.

SAP Note	Title	Comment
1501945	Secure Configuration SAP NW	This note contains information about how the NetWeaver platform can be configured securely.

Additional Information

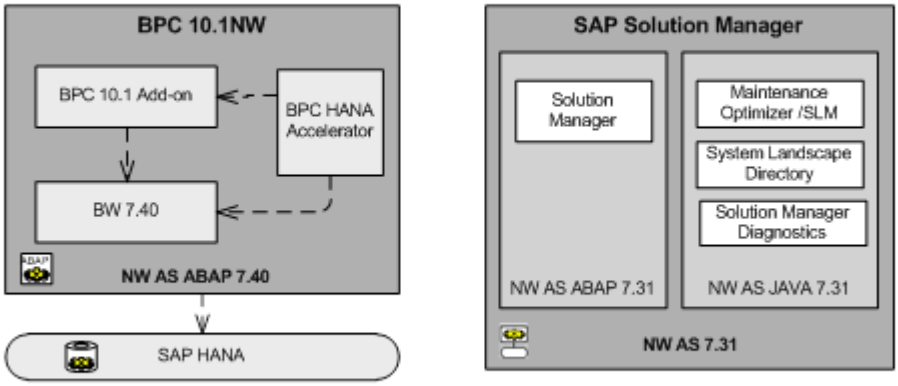
For more information about specific topics, see the Quick Links as shown in the table below.

Quick Links to Additional Information

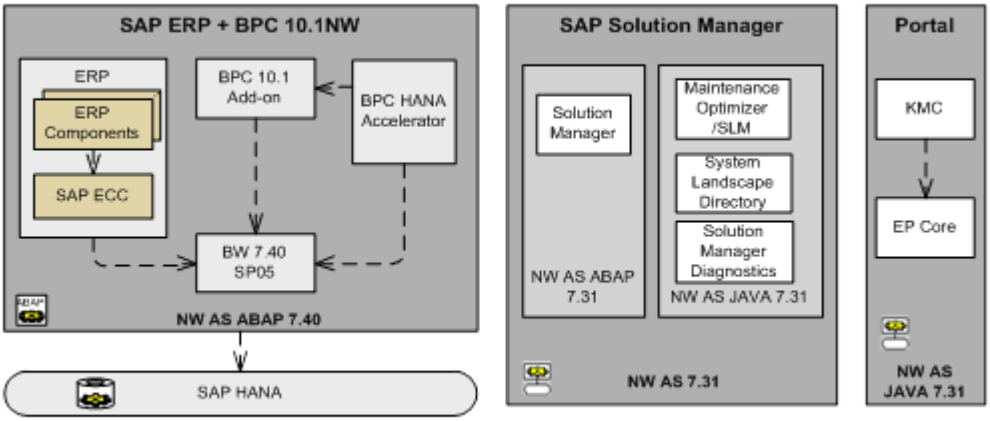
Content	Quick Link
Security	http://sdn.sap.com/irj/sdn/security
Security Guides	https://service.sap.com/securityguide
Related SAP Notes	https://service.sap.com/notes
Released Platforms	https://support.sap.com/pam
Network Security	https://service.sap.com/securityguide
SAP Solution Manager	https://service.sap.com/solutionmanager
SAP NetWeaver	http://sdn.sap.com/irj/sdn/netweaver

4 Technical System Landscape

Landscape for Planning and Consolidation Standard

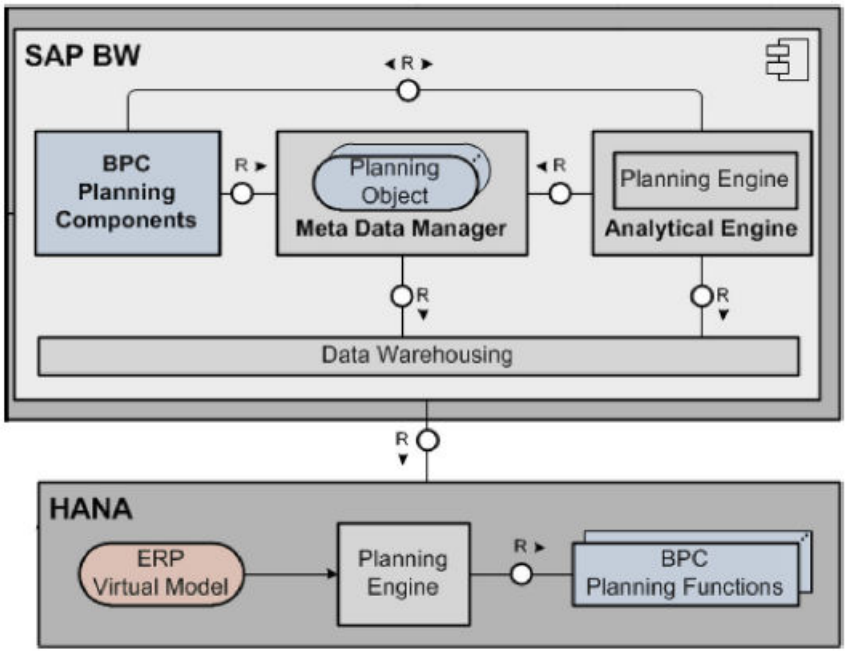


Planning and Consolidation Landscape in a Standard Configuration



Planning and Consolidation Landscape with SAP ERP System and Portal System Included

Landscape for Planning and Consolidation Embedded



Planning and Consolidation Landscape in an Embedded Configuration

For more information about the technical system landscape, see the Master Guide for the application on the SAP Help Portal.

5 Security Overview

Use

This section describes the security features included with Planning and Consolidation.

Features

Security Upon Initial System Installation

When you first install the system, the following items apply:

- The installation user can access the Administration workspace from any client machine. (After additional users are defined, they can also access the administration features remotely.)
- The system administrator can perform all administrative tasks, but does not have any access to members.
- There are no other users defined.

Standard only

- There are two Admin teams defined that can be used as samples.
- There is one sample task profile that has full Administration privileges (PrimaryAdmin), one sample task profile that has Public folder and dimension access (SecondaryAdmin), and another sample task profile that has privileges to manage the security settings, environments, and can use the system offline (SystemAdmin).
- Administrators must specifically assign task profiles to users or teams of users before they can access any tasks. Similarly, if they do not assign data access profiles to users or teams to define access to members of a secured dimension, no one has access to that dimension.

Steps to Define Security

Defining security involves the following steps:

- Manage users and roles with SAP NetWeaver Application Server ABAP user management mechanisms. See User Management [page 14].
- Configure integration into single sign-on environments. See Integration into Single Sign-On Environments [page 15].
- Optional: Assign users to teams. See Team Setup [page 17].
- Assign data access profiles to users or teams. See See Usage of Data Access Profiles (Standard only) [page 28] and Authorization Levels and Their Precedence (Embedded only) [page 35].

Standard only

- Name each user. See User Setup [page 16].
- Assign task profiles to users or teams. See Task Profile Setup [page 19].

Emergency User

When normal access to the system is no longer available, SAP customers can log on as `SysAdmin` (or other operating system users with administrative rights) to repair the Planning and Consolidation installation. For access to the ABAP server, see the *SAP NetWeaver Security Guide*.

Security Audit (Standard only)

All security-related changes, such as adding, changing, and deleting users, teams, task profiles and data access profiles can be audited by Planning and Consolidation.

> **i** Note
>
> The system stores all audit data in dynamically created internal tables, and does not create audit files in the back-end.

Administrators control whether activity auditing on administration tasks (including security tasks) is enabled or not. If enabled for administration tasks, all administration tasks are audited (see *Activity Auditing* in the application help for more information).

The following activities are audited by Planning and Consolidation:

- Adding, changing, and deleting users.
- Adding, changing, and deleting teams.
- Adding, changing, and deleting task profiles.
- Adding, changing, and deleting data access profiles.

Other events like successful or unsuccessful logins, locked users, and so on, are monitored by SAP NetWeaver.

To enable auditing for Administration tasks, you choose *Administration* and under the *Audit* section choose *Administration Activity* > *Enable Auditing of Administration Activity*. Once the system records an activity, you can run a report that shows activity based on specified criteria (see *Reporting on Administration Activity* in the help).

6 User Administration and Authentication

6.1 Introduction

The application uses the same user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide also apply to this.

For more information, see the SAP NetWeaver Application Server ABAP Security Guide on SAP Help Portal at http://help.sap.com *SAP NetWeaver* .

In addition to these guidelines, there is information about user administration and authentication that specifically applies to the application in the following sections:

- *User Management*
  This lists the tools to use for user management and the types of users required.
- *Integration into Single Sign-On Environments*
  This describes how the application supports Single Sign-On mechanisms.

This section also contains information about setting up users and teams in the following topics:

- Setting Up Users (Standard only) [page 16]
- Setting Up Teams [page 17]

6.2 User Management

Use

User management for the application uses the mechanisms provided with the SAP NetWeaver Application Server ABAP, for example, tools, user types, and password policies.

User Administration Tools

This table shows the tools to use for user management and user administration in the application.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance with SAP NetWeaver AS ABAP (Transactions SU01, PFCG)	For more information about user and role administration of AS ABAP, see SAP Help Portal at http://help.sap.com 	-

User Types

Planning and Consolidation

The user types required for the application include the following:

- Individual users
  - Dialog users are used for administration-related tasks.
  - Internet users are used by Flex client users.
- Technical users — not required

Standard Users

Planning and Consolidation

The application does not require the creation of additional dedicated users for any special purposes. Its use is possible via user accounts created for regular users by assigning the necessary application-related authorizations to them.

User Data Synchronization

The application does not deliver additional user data synchronization related features in addition to those available in the SAP NetWeaver platform. It also does not impose any special needs or restrictions, which would limit the usage of related NetWeaver tools.

> → Recommendation
>
> We recommend that the application is used in an environment where the same users exist throughout all the connected systems in the landscape.

6.3 Integration into Single Sign-On Environments

The application is capable of operating in any single sign-on environment supported by SAP NetWeaver out of the box, meaning there are no limitations imposed by the application on the possible single sign-on configurations within an SAP landscape. Refer to User Authentication and Single Sign-On section in the NW Security Guide for SSO setup. The supported mechanisms are as follows:

- Secure Network Communications (SNC)
- SAP Logon Tickets
- Client Certificates
- SAML 2.0

> **Note**
>
> SAML support is only available on SAP NetWeaver ABAP or Java 7.02 or higher.

- SPNego with Kerberos

For more information about the supported mechanisms, see SAP Help Portal at http://help.sap.com *SAP NetWeaver* .

SSO Ticket Validity and Web Session Expiration

When a user connects to the Planning and Consolidation web client, SAP NetWeaver not only creates a web session but also generates an SSO (single sign-on) ticket (in the MYSAPSSO2 cookie). This ticket has a default validity of 8 hours.

After session timeout, the web session correctly expires but the SSO ticket remains valid. If the user sends a new request after the session has expired, the system authenticates the user through SSO and creates a new session. From the user perspective, it appears that the session has not expired.

In order to have correct session expiration, the administrator must limit the validity period of the SSO ticket (for example, to two minutes, which is the validity period of reentrance tickets). You set this using the kernel parameter `login/ticket_expiration_time` in the SAP NetWeaver `default.pfl` configuration file, for example, `login/ticket_expiration_time=0:02`.

For more information about how to set this parameter, see the SAP NetWeaver help at http://help.sap.com/saphelp_nw74/helpdata/en/22/41c43ac23cef2fe10000000a114084/content.htm.

6.4 Setting Up Users (Standard only)

Use

You can add new users in an environment and assign them to teams, task profiles, and data access profiles.

If you are not using the default task or data access profiles and have not set them up yet, we recommend that you define them before adding users. You might also want to create teams, so that you can assign the newly added users to the appropriate teams.

Alternatively, when you define the teams and profiles, you can assign users to them at that time.

> **Note**
>
> Sarbanes-Oxley compliance is a hardcoded behavior in Planning and Consolidation, as the system does not save users' passwords on client machines.

Features

Adding Users

Before you can add a new user, you must have created that user in the ABAP back-end. For more information, see the SAP NetWeaver Security Guide.

To add users, go to *Administration* and under the *Security* section, choose *Users*. In the Users view, select *Add*. In the *Add User* assistant, select the one or more users to add in the environment and assign one or more teams to the users.

Modifying Users

To modify a user definition, go to *Administration* and under the *Security* section, choose *Users*. In the Users view, highlight the user and select *Edit*. You can then add or remove teams, task profiles and data access profiles for the user.

Removing Users

To remove an existing user, go to *Administration* and under the *Security* section, choose *Users*. In the Users view, highlight the user and select *Remove*, then click *OK*.

6.5 Setting Up Teams

Use

You can set up and maintain teams of users. When you assign security to a team, the security works collectively on the team members. This allows you to set up task and data access security for several users at the same time. Teams are not required to successfully process security.

Features

Adding Teams

To add teams, go to *Administration* and under the *Security* section, choose *Teams*. In the Teams view, select *New*. In the *Add Team* assistant, enter an ID and a description for the team and assign one or more users to it.

Modifying Teams

To add teams, go to *Administration* and under the *Security* section, choose *Teams*. In the Teams view, highlight the team and select *Edit*. You can then add or remove users, task profiles and data access profiles for the team.

Removing Teams

To add teams, go to *Administration* and under the *Security* section, choose *Teams*. In the Teams view, highlight the team and select *Delete*, then click *OK*.

Assigning Team Leaders

Assigning one or more team leaders is useful when you want to give them special access rights to the team's folder. You can assign team leaders while you are defining or modifying a team. You can choose one or more team members to be a team leader.

7 Authorizations

7.1 Introduction

The application uses the classic authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver Application Server ABAP Security Guide also apply to the application.

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG).

To define the models and data within those models to which users have access, you can use data access profiles in both the standard and embedded configurations of Business Planning and Consolidation. For detailed steps, refer to Data Access Profile Setup (Standard only) [page 27] and Authorization Levels and Their Precedence (Embedded only) [page 43].

To define what types of activities or tasks a user is authorized to perform in different functions, you can leverage the SAP NetWeaver authorization concept:

- In Business Planning and Consolidation in an embedded configuration, you assign authorization objects to users based on roles.
- In Business Planning and Consolidation in a standard configuration, you assign task profiles to users or a team of users in the web client.

For more information about how to maintain roles, see the SAP NetWeaver role administration information on the SAP Help Portal at http://help.sap.com.

7.2 Task Profile Setup (Standard only)

Use

A task profile defines the type of activities or tasks an administrator, a user, or a team of users can perform in the system.

Features

Planning and Consolidation is installed with three administrative task profiles by default. You cannot modify these default profiles. You can, however, copy these profiles to create additional profiles for users and teams.

Administrator Task Profiles

The following default administrative task profiles permit a specific set of tasks:

- SystemAdmin
- PrimaryAdmin
- SecondaryAdmin

A System Administrator (SystemAdmin), by default, has the following task rights:

- Manage Environments
- Manage Security
- Use System When Offline

A Primary Administrator (PrimaryAdmin), by default, has the following task rights:

- Manage Models
- Manage Business Rules
- Manage Dimensions
- Manage Data Locks and Work Status
- Manage Environment Status
- Manage Drill Throughs
- Manage Templates
- Manage Audit
- Use Offline Distribution
- Edit Comments
- Edit Book and Distribution templates
- Publish Books
- Run Documents from EPM add-in
- Manage Security
- Administer Documents

A Secondary Administrator (SecondaryAdmin), by default, has the following task rights:

- Manage Dimensions
- Edit content of Public Folder

If you want a user to perform administration tasks, you must assign them one of the predefined administrator roles. Without one of these roles, the user cannot perform any administrator tasks.

The following tables provide the tasks, organized by functional area of the system, that administrators can assign to users and teams.

Administration Task Profile Descriptions

The following table describes the available tasks in the *Administration* interface:

Task	Can be assigned to	Description
Manage Business Rules	Primary administrator	Can define business rules.
Manage Data Locks and Work Status	Primary administrator	Can define and edit work status codes.
Manage Dimensions	Primary and secondary administrators	Create, modify, process, and delete dimensions and members.

Task	Can be assigned to	Description
Manage Document Types	Any user or team	Can categorize collaboration postings, which is useful when filtering collaboration postings to see certain types. Subtypes can be managed by administrators or created by users as they post.
Manage Drill Throughs	Primary administrator	Can create and modify drill-through setup.
Manage Environment Status	Primary administrator	Can view environment status.
Manage Environments	System administrator	Can create and modify environments, and set environment parameters.
Manage Models	Primary administrator	Can create, modify, and delete models in an environment, make changes to dimensions, add dimensions, optimize models, and manage logic scripts.

Analysis and Collection Task Profile Descriptions

The following table describes the available tasks in the *Analysis and Collection* interface:

Task	Can be assigned to	Description
Manage Templates	Any user or team	Can access templates from the public folder, and restrict workbook options. A team member or team leader with this task can access and save templates to their respective team folder.
Run Drill Throughs	Any user or team	Can execute drill-throughs.
Use Input Forms and Save Data	Any user or team	Can access the built input schedules and send data. Can use spread, weight, and trend options. Controls submitting data from the web reports.

Audit Task Profile Descriptions

The following table describes the available tasks in the *Audit* interface:

Task	Can be assigned to	Description
Manage Audit	Any user or team	Can manage activity and data auditing.

Business Process Flows Task Profile Descriptions

The following table describes the available tasks in the *Business Process Flows* interface:

Task	Can be assigned to	Description
Manage BPFs	Any user or team	Can create, modify, and delete business process flows.
Use BPFs	Any user or team	Can execute business process flow tasks.

Collaboration Task Profile Descriptions

The following table describes the available tasks in the *Collaboration* interface:

Task	Can be assigned to	Description
Use Offline Distribution	Any user or team	Can use the Offline Distributor.
Use Offline Collection	Any user or team	This user or team collects changes to offline input schedules and sends data to a database.

Comments Task Profile Descriptions

The following table describes the available tasks in the *Comments* interface:

Task	Can be assigned to	Description
Administer Comments	Any user or team	Can add, modify, and remove comments for all users.
Edit Comments	Any user or team	Can add, modify, and remove his or her own comments.

Consolidations Task Profile Descriptions

The following table describes the available tasks in the *Consolidations* interface:

Task	Can be assigned to	Description
Dismiss Blocking Controls	Any user or team	Can force failing controls to Dismissed status
Edit Ownership Manager	Any user or team	This user or team has write access to the Ownership Manager, but cannot run the ownership calculation routine.
Edit Controls definition	Any user or team	Can set up controls in Administration.

Task	Can be assigned to	Description
Reset Control Dismissal	Any user or team	Can reset a Dismissed control status to its previous status.
View Consolidation Monitor	Any user or team	Can access the Consolidation Monitor, but cannot perform any actions.
Run Consolidation Tasks	Any user or team	Can run currency translation and consolidations in the Consolidation Monitor.
Run Controls	Any user or team	Can access Controls Monitor and run control calculations.
Run Ownership Calculations	Any user or team	Can execute the ownership calculation.
View Controls	Any user or team	Can access Controls Monitor in read-only mode.
View Controls definition	Any user or team	Can read Control Manager definitions.
View Ownership Manager	Any user or team	Can access the landing page of the Ownership Manager.

Data Manager Task Profile Descriptions

The following table describes the available tasks in the *Data Manager* interface:

Task	Can be assigned to	Description
Run Admin Packages	Any user or team	Can run Admin packages within Data Manager.
Edit Packages	Any user or team	Can maintain packages within Data Manager.
Edit Transformation Files	Any user or team	Can maintain transformation files within Data Manager.
Edit Conversion Files	Any user or team	Can maintain conversion files within Data Manager.
Cancel Any User Packages	Any user or team	Can cancel user packages within Data Manager.
Edit Package Schedules for any user	Any user or team	Can change the package schedule for any user within Data Manager.
Run Packages	Any user or team	Can run packages within Data Manager.

Task	Can be assigned to	Description
Edit Package Links	Any user or team	Can maintain package links within Data Manager.
Upload Data	Any user or team	Can upload data within Data Manager.
Download Data	Any user or team	Can download data within Data Manager.

Folder Access Task Profile Descriptions

The following table describes the available tasks in the *Folder Access* interface:

Task	Can be assigned to	Description
Edit content of Public Folders	Secondary Admin	Can add and manage content in the public folder, including creating new folders. User also needs document type access rights, such as Edit Workspaces or Edit Reports.

Journal Task Profile Descriptions

The following table describes the available tasks in the *Journal* interface:

Task	Can be assigned to	Description
Edit Journals	Any user or team	Can create or modify journal entries.
Lock/Unlock Journals	Any user or team	Can lock and unlock journal entries
Manage Journals	Any user or team	Can manage journals as follows: • Create and maintain journal templates • Clear journal tables • Create Journal
Post Journals	Any user or team	Can post journals.
View Journals	Any user or team	Can view journals.
Unpost Journals	Any user or team	Can unpost journal entries.
Reopen Journals	Any user or team	Can reopen journals.

Publish Task Profile Descriptions

The following table describes the available tasks in the *Publish* interface:

Task	Can be assigned to	Description
Edit Book and Distribution templates.	Primary Admin	Can create, edit, and save book and distribution templates.
Publish Books	Primary Admin	Can publish a book of reports.
Run Documents from EPM add-in	Primary Admin	Can run documents from the EPM Add-in for Microsoft Office.

System Reports Task Profile Descriptions

The following table describes the available tasks in the *System Reports* interface:

Task	Can be assigned to	Description
Run Audit Reports	Any user or team	Can run audit reports.
Run Comment Reports	Any user or team	Can run a comment report.
Run Security Reports	Any user or team	Can run security reports.
Run Work Status Reports	Any user or team	Can run a work status report.

System Security Task Profile Descriptions

The following table describes the available tasks in the *System Security* interface:

Task	Can be assigned to	Description
Use System When Offline	System Admin	Can log onto Planning and Consolidation when the status of an environment is *Not Available*.
Manage Security	System and primary administrators	Can manage users, task, and data access profiles. **⚠ Caution** We recommend that you restrict access of this task to a few privileged users.

Web Report Task Profile Descriptions

The following table describes the available tasks for web reports:

Task	Can be assigned to	Description
Edit Documents	Any user or team	User can use documents, can add, edit, and delete their own documents, and can access all documents shared with them.
Edit Reports	Primary Administrator	User can create web reports, and can open and edit their web reports and those of other users. Gives these rights in all folders the user has write access.
Administer Documents	Primary Administrator	Can use documents, and can add, edit, and delete all documents.
Edit Workspaces	Any user or team	Can create and update workspaces.
Edit Crystal Dashboards	Any user or team	Can create and modify, and save Crystal Dashboards.

Web Service Task Profile Descriptions

The following table describes the available tasks in the *Web Service* interface:

Task	Can be assigned to	Description
Access BPC from FIM and SSM	Any user or team	Can access Planning and Consolidation from the Financial Information Management and Strategy Management applications.

Work Status Task Profile Descriptions

The following table describes the available tasks in the *Work Status* interface:

Task	Can be assigned to	Description
Use Work Status	Any user or team	Can change the work status on a data region.

Adding a Task Profile

To create a new task profile in the Administration workspace, choose *Security* > *Task Profiles* > *New*. Enter data as required.

Tips for Assigning Task Profiles

- The number of task profiles administrators can assign to a user is not limited. However, we recommend that you do not assign multiple task profiles to users because it may cause you confusion in determining their ultimate access rights.
  Task access security is cumulative, and tasks cannot be explicitly denied. As a result, assigning multiple task profiles can create a situation where users have access to tasks that you may not want them to have.
- Administrators can assign multiple task profiles to a team. However, we recommend that you do not assign multiple task profiles to a team because it may cause you confusion in determining the ultimate access rights of that team.

7.3 Data Access Profile Setup (Standard only)

Use

You must define a data access profile for all secured dimensions of a model. If no profile is defined for a secured dimension, the users assigned to the profile do not have access rights to that model. If you partially define access, for example, for one of two secured dimensions, users are still denied access to the model.

After creating a data access profile, you assign it to users as needed.

Features

General Rules for Data Access Security

Data access security is based on the following rules:

- By default, no one other than the system administrator has access to members. Member access must be explicitly granted.
- A user can be assigned data access individually and through team membership.
- Data access privileges flow down the hierarchy, from parent to child.
- When in conflict, the least restrictive data access profile is applied.
- In case of a conflict between individual and team data access, the least restrictive setting is applied.

Creating Data Access Profiles

1. Go to the *Administration* page and under the *Security* section, choose *Data Access Profile*.
2. On the screen that appears, choose *New*.
3. Enter the ID and description of the new data access profile.
4. Select the required model from the list.
5. For each authorization relevant dimension, select the required members and set their access rights.
6. Go to the *Users* or *Teams* tab to assign the new data access profile to users that are assigned to the current environment or teams that have corresponding users assigned to it.

Defining Access to Members with Children

When defining access to a secured dimension that has one or more defined hierarchies, security is applied to the member and all of its children. For example, if you grant access to a member that has 10 children, users with access to the parent member also have access to the 10 children.

You can restrict a child member of a parent with 'Read Only' or 'Write' access by creating a separate data access profile and assigning the child 'Denied' access. Alternatively, you can use the same data access profile as the parent, but create a new line item for the child.

Resolving Data Access Profile Conflicts

Since you can define member access by individual users and by teams, there may be situations in which conflicts occur. The following sections describe some potential member access conflict scenarios and the rules the system applies to resolve those conflicts. These scenarios are based on the assumption that the Entity dimension is a secured dimension and has the following hierarchical structure:

Hierarchy	Members			
H1	WorldWide1	Sales	SalesAsia	SalesKorea
				SalesJapan
				ESalesAsia
			SalesEurope	SalesItaly
				SalesFrance
				ESalesEurope
H2	WorldWide2	Asia	Korea	SalesKorea
			Japan	SalesJapan
			eAsia	ESalesAsia
		Europe	Italy	SalesItaly
			France	SalesFrance
			eEurope	ESalesEurope

Conflict Between Profiles

When there is a conflict between data access profiles, the least restrictive profile is always applied. This section describes three different scenarios where there are conflicts between profiles.

Example

Scenario 1:

- User1 belongs to Team1 and Team2.
- There are two data access profiles: ProfileA and ProfileB.
- ProfileA is assigned to Team1 and ProfileB is assigned to Team2.

The data access profiles are described in the following table:

Data Access Profile	Access	Dimension	Member
ProfileA	Write	Entity	Sales

ProfileB	Read Only	Entity	SalesAsia

In this case, the least restrictive profile between the two, ProfileA (Write), is applied. As a result, ProfileB is ignored by the system, and User1 is able to send data to both SalesKorea and SalesItaly.

Example

Scenario 2:

- User1 belongs to Team1 and Team2
- There are two data access profiles: ProfileA and ProfileB.
- ProfileA is assigned to Team1 and ProfileB is assigned to Team2.

The data access profiles are described in the following table:

Data Access Profile	Access	Dimension	Member
ProfileA	Read Only	Entity	Sales
ProfileB	Write	Entity	SalesAsia

In this case, the least restrictive profile between the two, ProfileB (Write), is applied for the child members of SalesAsia. As a result, ProfileA is ignored by the system, and User1 is able to send data to SalesKorea, but not to SalesItaly.

Example

Scenario 3:

- User1 does not belong to any team.
- There are two data access profiles: ProfileA and ProfileB.
- Both the profiles are assigned to the user.

The data access profiles are described in the following table:

Data Access Profile	Access	Dimension	Member
ProfileA	Denied	Entity	SalesAsia
ProfileB	Read Only	Entity	Sales

In this case, the least restrictive profile between the two, ProfileB (Read Only), is applied. As a result, ProfileA is ignored by the system, and User1 is able to retrieve data from both SalesKorea and SalesItaly.

Conflict Between Parent and Child Members

Authority always flows down the hierarchy from parent to child. Child members always have the access level of their parents, unless otherwise specified.

Example

Scenario 1:

- User1 belongs to Team1 and ProfileA is assigned to Team1.
- Two levels of data access profiles are defined for ProfileA.

The data access profiles for ProfileA are described in the following table:

Data Access Profile	Access	Dimension	Member
ProfileA	Write	Entity	Sales
ProfileA	Read Only	Entity	SalesAsia

In this case, the Write access of the Sales member flows down to its children. This flow is interrupted by assigning Read Only access to SalesAsia (a descendant of Sales), and SalesAsia's access flows down to its descendants. As a result, User1 is able to send data to SalesItaly, but not to SalesKorea.

Example

Scenario 2:

- User1 belongs to Team1 and ProfileA is assigned to Team1.
- ProfileA has two levels of data access profiles.

The data access profiles for ProfileA are described in the following table:

Data Access Profile	Access	Dimension	Member
ProfileA	Read Only	Entity	Sales
ProfileA	Write	Entity	SalesAsia

In this case, the Read Only access of the Sales member flows down to its children. This flow is interrupted by assigning Write access to SalesAsia (a descendant of Sales), and SalesAsia's access flows down to its descendants. As a result, User1 is able to send data to SalesKorea but not to SalesItaly.

Conflict When the Same Member Belongs to Different Hierarchies

When a member belongs to different hierarchies, and there is a conflict in member access, the most restrictive access is applied.

Example

Scenario: ProfileA and ProfileB are assigned to User1. The data access profiles are described in the following table:

Data Access Profile	Access	Dimension	Member
ProfileA	Read Only	Entity	WorldWide1

ProfileB	Write	Entity	WorldWide2

In this case, ProfileB determines User1's access. As a result, User1 is able to send data to SalesKorea, even if ProfileA denies User1 Write access to SalesKorea (in WorldWide1 hierarchy).

Attribute Based Data Access Profiles

When you are creating a data access profile, you can assign different levels of access based on properties. The examples described below are based on the following hierarchy:

ID	Region	Country	Currency
Entity0	Europe	Germany	Euro
— Entity1	Europe	Germany	Euro
— — Entity101	Europe	UK	GBP
— — Entity102	Europe	France	Euro
— — Entity103	Europe	Germany	Euro
— Entity2	North America	USA	USD
— — Entity201	North America	USA	USD
— — Entity202	North America	Canada	CAD
— — Entity203	North America	Mexico	MXN

Example — One Data Access Profile

The data access profile DAP1 is defined as follows:

Rule Number	Members	Access	Comment	Result
1	Entity1	Read	Read access to Entity1 and all its descendants	Read access to Entity1, Entity101, Entity102, Entity103
2	Country = Germany and Currency = Euro	Write	Write access to members whose Country is Germany and Currency is Euro	Write access to Entity0, Entity1 and Entity103
3	Entity103	Deny	No access to Entity103	No access to Entity103

When there are conflicting rules in a data access profile, the priority is as follows (from highest to lowest):

1. Access defined exactly on the member (be it a base member or a parent member).
2. Access defined by attributes (will not be inherited).

> **Example**
>
> If the defined attributes are `Currency=Euro: Read` and `Country=France: Write`, then Entity102 is writable.

3. Access inherited from parent.
4. Access defined to “All members” (as if defined on a virtual parent on top of the hierarchy).

The result is shown in the table below:

ID	Access	Comment
Entity0	Write	Defined by rule number 2.
Entity1	Read	Read access defined by rule number 1; Write access defined by rule number 2. Rule number 1 is applied, because it applies directly to Entity1.
Entity101	Read	Defined by rule number 1.
Entity102	Read	Defined by rule number 1.
Entity103	Deny	Read access defined by rule number 1; Write access defined by rule number 2; Deny access defined by rule number 3. Rule number 3 is applied, because it applies directly to Entity103.
Entity2	Deny	If no rules exist, access is denied by default.
Entity201	Deny	If no rules exist, access is denied by default.
Entity202	Deny	If no rules exist, access is denied by default.
Entity203	Deny	If no rules exist, access is denied by default.

Example — Two Data Access Profiles

Data access profile DAP2 is defined as follows:

Rule Number	Members	Access	Comment	Result
1	All members	Read	Read access to all members	Read access to all members

Rule Number	Members	Access	Comment	Result
2	Entity1	Deny	No access to Entity1 and its descendants	No access to Entity1, Entity101, Entity102 and Entity103
3	Currency = USD	Write	Write access to members whose currency is USD	Write access to Entity2 and Entity201

The result of this data access profile is shown in the table below:

ID	Access	Comment
Entity0	Read	Defined in rule number 1.
Entity1	Deny	Read access defined by rule number 1; Deny access defined in rule number 2. Rule number 2 is applied, because it applies directly to Entity1 and its descendants.
Entity101	Deny	Read access defined by rule number 1; Deny access defined in rule number 2. Rule number 2 is applied, because it applies directly to Entity1 and its descendants.
Entity102	Deny	Read access defined by rule number 1; Deny access defined in rule number 2. Rule number 2 is applied, because it applies directly to Entity1 and its descendants.
Entity103	Deny	Read access defined by rule number 1; Deny access defined in rule number 2. Rule number 2 is applied, because it applies directly to Entity1 and its descendants.
Entity2	Write	Read access defined by rule number 1; Write access defined in rule number 3. Rule number 3 is applied, because it applies directly to the properties of Entity 2.

ID	Access	Comment
Entity201	Write	Read access defined by rule number 1; Write access defined in rule number 3. Rule number 3 is applied, because it applies directly to the properties of Entity 201.
Entity202	Read	Defined by rule number 1.
Entity203	Read	Defined by rule number 1.

If several data access profiles are assigned to a user or a team, the combination of the least restrictive rules of all profiles is applied. Therefore, if both DAP1 and DAP2 are assigned to a user, that user will have the following permissions:

ID	Access granted by DAP1	Access granted by DAP2	Result
Entity0	Write	Read	Write access
Entity1	Read	Deny	Read access
Entity101	Read	Deny	Read access
Entity102	Read	Deny	Read access
Entity103	Deny	Deny	Access denied
Entity2	Deny	Write	Write access
Entity201	Deny	Write	Write access
Entity202	Deny	Read	Read access
Entity203	Deny	Read	Read access

7.4 Integrating with Central User Authorization

Central user authorization (CUA) is a system separate from Business Planning and Consolidation that is responsible for user authorization activities such as controlling data access.

After enabling this feature and creating a data access profile in Business Planning and Consolidation, no corresponding roles are generated on the NetWeaver server. Instead, you need to create a related role in the CUA system to be used for further authorization checks.

For detailed information, refer to SAP Note 1880183 - Support create profile and assign user in CUA enabled system (standard mode) or 2157598 - Support create data access profile in CUA enabled system (embedded mode).

For instructions about how to set up central user authorization, refer to the help topic “Central User Authorization” at http://help.sap.com/saphelp_nw70ehp2/helpdata/en/bf/b0b13bb3acd607e10000000a11402f/content.htm.

7.5 Authorization Objects (Embedded only)

In the Business Planning and Consolidation embedded configuration, you assign authorization objects to users based on roles by leveraging the profile generator (transaction PFCG) tool of BW/4HANA.

Related Information

Authorization Objects for SAP Business Explorer [page 35]
Authorization Objects for Administration (Embedded only) [page 36]
Authorization Objects for Maintaining Data Access Profile (Embedded only) [page 38]
Authorization Objects for Modeling (Embedded only) [page 38]
Authorization Objects for Reporting and Planning (Embedded only) [page 40]
Authorization Objects for Performing Consolidation Tasks (Embedded only) [page 42]

7.5.1 Authorization Objects for SAP Business Explorer

For reporting through SAP Business Explorer (BEx), users must log on to the SAP backend system. Authorization objects for each user must be maintained in that system.

The following table describes the authorization objects that are required.

Authorization Object	Technical Name	Description
BEx – Components	S_RS_COMP	Authorization for using different components for the query definition
BEx – Components	S_RS_COMP1	Authorization for queries from specific owners
BEx – Components	S_RS_FOLD	Display authorization for folders
BEx – Individual Tools	S_RS_TOOLS	Authorization for individual Business Explorer tools
BEx – Enterprise Reports	S_RS_ERPT	Authorization for BEx enterprise reports

Authorization Object	Technical Name	Description
BEx – Enterprise Report Reusable Elements	S_RS_EREL	Authorization for reusable elements of a BEx enterprise report
BEx – Data Access Services	S_RS_DAS	Authorizations for working with data access services
BEx – Web Templates	S_RS_BTMP	Authorization for working with BEx Web templates
BEx – Reusable Web Items	S_RS_BITM	Authorization for working with BEx Web items
BEx Information Broadcasting Authorization for Scheduling	S_RS_BCS	Authorization for registering broadcast settings for execution
BEx Texts (Maintenance)	S_RS_BEXTX	Authorization for maintaining BEx texts

To maintain the authorization objects for users, proceed as follows:

1. Enter transaction `PFCG` to create or edit a role definition.
2. Assign one or more authorization objects to the role in the role definition.
3. Assign the role to specific users in this transaction. You can also choose to append the role to a user profile in transaction `SU01`.

7.5.2 Authorization Objects for Administration (Embedded only)

Enter transaction `SU21` to view an authorization object's definition, including its description, authorization fields, and permitted activities. The table below lists the administration-related authorization objects available for Planning and Consolidation in an embedded configuration taken from the T-code.

Authorization Object	Technical Name	Description	Field 1	Field 2	Field 3	Activity
Identity	RSBPC_ID	Grants the user access to an environment	Environment Name	-	-	-
Environment	RSBPC_ENVM	Manage environment	Environment Name			Maintain (includes create, change and delete), Display

Authorization Object	Technical Name	Description	Field 1	Field 2	Field 3	Activity
Model	RSBPC_MODL	Manage model	Environment Name	Model Name	-	Maintain, Display, Change status (Change work status), Execute (use model)
BPF	RSBPC_BBPF	Manage and use BPF	Environment Name	BPF template name	-	Maintain, Display, Administer (administration of a BPF instance), Execute (use BPF)
Team	RSBPC_TEAM	Manage Team	Environment name	Team name	-	Maintain, Display
Resource	RSBPC_WKSP	Resource management (workbook, web report, and so on)	Environment name	Resource type	Folder	Maintain (includes create, change and delete), Display
User	RSBPC_USER	Manage users	Environment	User ID	-	Maintain, Display
Data Access Profile	Data Access Profi-leRSBPC_DAP	Manage data access profiles	Environment	Profile ID	-	Maintain, Display

To maintain the authorization objects for users, proceed as follows:

1. Enter transaction `PFCG` to create or edit a role definition.
2. Assign multiple authorization objects, for example, `RSBPC_ENVM` and `RSBPC_MODL` to the role in the role definition, with specified activity values in the corresponding authorization fields.
3. Assign the role to specific users in this transaction. You can also choose to append the role to a user profile in transaction `SU01`.

7.5.3 Authorization Objects for Maintaining Data Access Profile (Embedded only)

To maintain a data access profile for a user or a team in the embedded configuration, users must first have been assigned the proper authorization with the following authorization objects:

Authorization Object	Description	Field 1	Field 2	Activity
S_USER_GRP	Get user's roles at runtime	CLASS	ACTVT	Create, Change, Display, Delete
S_USER_AGR	Manage roles	ACT_GOUP	ACTVT	Create, Generate, Change, Display, Delete, Transport
S_USER_PRO	Manage authorization profiles	PROFILE	ACTVT	Create, Change, Display, Delete
S_USER_VAL	Restrict values that can be changed for a role	OBJECT: If a user wants to maintain organizational levels in a role, the complete authorization ("*") should be assigned for this authorization field.	AUTH_FIELD AUTH_VALUE: If a user wants to maintain intervals or use generic entries, the user must have the full authorization ("*") for this field.	None

To maintain the authorization objects for users, follow these steps:

1. Enter transaction `PFCG` to create or edit a role definition.
2. Assign authorization objects with specified activity values in the corresponding authorization fields.
3. Assign the role to specific users in this transaction. You can also choose to append the role to a user profile in transaction `SU01`.

7.5.4 Authorization Objects for Modeling (Embedded only)

Maintaining Central and Local Master Data

To maintain **master data** for a given dimension, users must have proper authorization for the master data with authorization object `S_RS_IOMAD` and corresponding activities:

- Activity 03 - View dimension structure and view dimension member
- Activity 23 - Maintain dimension member
- Activity 06 - Delete dimension member

To maintain **local master data**, users must have proper authorization with authorization object `S_RS_ADMWB`, `S_RS_IOBJ`, and `RSBPC_IOMA`. Each of them needs to be maintained with corresponding activities.

For `S_RS_ADMWB`, assign:

- Activity 03 - Display Data Warehousing workbench InfoObject
- Activity 16 - Execute Data Warehousing workbench InfoObject

For `S_RS_IOBJ`, assign:

- Activity 03 - Display
- Activity 23 - Maintain

For `RSBPC_IOMA`, assign:

- Activity 03 - Display local master data
- Activity 23 - Maintain local master data

Creating and Maintaining Local InfoProviders

To maintain local InfoProviders for a given model, users must have proper authorization for the InfoProvider with authorization object `S_RS_WSPAC`, `S_RS_AINX`, `S_RS_ALVL`, and `S_RS_PLSE`. Each of them needs to be maintained with corresponding activities.

For `S_RS_WSPAC`, assign:

- Activity 03: Display
- Activity 16: Execute

For `S_RS_AINX`, assign:

- Activity 03: Display analytic index

For `S_RS_ALVL`, assign:

- Activity 03: Display aggregation level

For `S_RS_PLSE`, assign:

- Activity 03: Display planning function
- Activity 16: Execute planning function

Maintaining Central and Local Hierarchies

To maintain the **central** hierarchy for a given dimension, users must have proper authorization with authorization object `S_RS_HIER` and corresponding activities:

- Activity 03: Display central hierarchy
- Activity 23: Maintain central hierarchy

To maintain the **local** hierarchy for a given dimension, users must have proper authorization with authorization object `S_RS_WSPAC` and `RSBPC_LOHE`. Each of them needs to be maintained with corresponding activities.

For `S_RS_WSPAC`, assign:

- Activity 03: Display BW workspace
- Activity 16: Execute BW workspace

For `RSBPC_LOHE`, assign:

- Activity 03: Display local hierarchy
- Activity 23: Maintain local hierarchy

7.5.5 Authorization Objects for Reporting and Planning (Embedded only)

In the embedded configuration of Planning and Consolidation, users need to have the following authorization objects to perform reporting and planning activities:

Running Global Queries

To run global queries, users must have proper authorization with authorization object:

S_RS_AUTH: BI Analysis Authorizations in Role

`S_RS_COMP` assigned with:

- Activity 03 - Display Business Explorer components
- Activity 16 - Execute Business Explorer components

`S_RS_COMP1` assigned with:

- Activity 03 - Display Business Explorer components
- Activity 16 - Execute Business Explorer components

Creating or Maintaining Local Queries

To create and maintain local queries, users must have proper authorizations with authorization object:

`S_RS_ADMWB` assigned with:

- Activity 03 - Display Data Warehousing Workbench
- Activity 16 - Execute Data Warehousing Workbench

`S_RS_ALVL` assigned with:

- Activity 03 - Display aggregation level
- Activity 23 - Maintain aggregation level

S_RS_AUTH: BI Analysis Authorizations in Role

`S_RS_COMP` assigned with:

- Activity 03 - Display Business Explorer components
- Activity 16 - Execute Business Explorer components

`S_RS_COMP1` assigned with:

- Activity 03 - Display Business Explorer components
- Activity 16 - Execute Business Explorer components

`S_RS_COPR` assigned with:

- Activity 02 - Change local CompositeProvider

`S_RS_HIER` assigned with:

- Activity 03 - Display Data Warehousing Workbench hierarchy
- Activity 71 - Analyze Data Warehousing Workbench hierarchy

`S_RS_IOBJ` assigned with:

- Activity 03 – Display InfoObject

S_RS_WSPAC assigned with:

- Activity 16 - Execute BW workspace
- Activity 68 - Model

S_USER_GRP assigned with:

- Activity 03 - Display user group

S_ADT_RES: ABAP Development Tool Resource Access

Carrying Out Reporting and Planning Activities

To carry out reporting and planning based on local queries, users must have proper authorizations with authorization objects:

S_CTS_ADMI: Administration functions for changing and transporting system

S_CTS_SADM: System-specific administration (transport)

S_RS_WSPAC assigned with:

- Activity 03 - Display BW workspace
- Activity 16 - Execute BW workspace

Redirecting from BPF to Analysis Office

To redirect to an AO workbook from a business process flow, users must have proper authorizations with authorization object S_RFC with:

- Activity 16: Execute authorization check for RFC access

Working with System Reports

To enable or disable data changes in a certain InfoProvider by each model, users must be assigned the authorization object S_RS_ICUBE with:

- Activity 03: Display InfoCube

After that users can make such changes in the web client via *Administration* > *Audit* > *Data Changes*.

To view the *System Reports* page, users must be assigned the authorization object S_RS_COMP with:

- Activity 16: Execute
- RSZCOMPTP REP: Query

To execute all system reports, users must have proper authorizations with authorization object:

S_RS_COMP1 assigned with:

- Activity 16: Execute
- RSZCOMPTP REP: Query

S_RS_AUTH assigned with:

- BUIAUTH 0BI_ALL: make analysis authorizations available

7.5.6 Authorization Objects for Performing Consolidation Tasks (Embedded only)

To view and execute consolidation-related tasks, users must have proper authorization to manage controls, journals, Consolidation Monitor, and ownership, which you can set up by following the steps listed below.

If you do not intend to perform consolidation-related functions in Business Planning and Consolidation, installation of these authorization objects is not required.

1. Enter transaction `SU21` to view authorization object definitions, including its description, authorization fields, and permitted activities. For example, the following table shows the detailed information of consolidation-related authorization objects taken from the T-code.

Authorization Object	Technical Name	Description	Activity
Manage Control	`RSBPC_CTR`	Authorization object that is checked during actions related to Controls.	Field name: ACTVT ○ 03-Display: Display control rule ○ 16-Execute: Execute controls from the controls monitor ○ 23-Maintain: Maintain control rules ○ GL-General Overview: View Control and controls results from controls monitor Field name: RSBPCCTACT ○ DS-Dismiss Control ○ EX-Execute Control ○ RS-Reset Control
Manage Journal	`RSBPC_JNL`	Authorization object that is checked during actions related to Journals.	23-Maintain Journal Template GL-Display Journal Template 02-Maintain Journal: Create and edit journals 03-Display Journal: View journals 05-Lock/Unlock Journals 10-Post Journal 85-Unpost Journal C5-Re-open Journal

Authorization Object	Technical Name	Description	Activity
Manage Consolidation Monitor	RSBPC_MON	Authorization object that is checked when the consolidation task sequence or status is viewed or maintained.	03-Display (view consolidation monitor and status) 23-Maintain (define task sequence) GL-General Overview (display task sequences in consolidation monitor)
Manage Ownership	RSBPC_OWN	Authorization object that is checked when ownership manager is viewed or maintained.	03-Display 23-Maintain (all steps except triggering ownership calculation) 93-Calculate (ownership calculations)
Manage Business Rules	RSBPC_RUL	Authorization object this is checked when defining a business rule and executing business rules from consolidation monitor	23-Maintain (maintain business rules) 03-Display (view business rules) 16-Execute (Trigger consolidation tasks from consolidation monitor. Display the running process, refresh status, and reset status in Consolidation Monitor.)

2. Enter transaction PFCG to create/edit a role definition.
3. Assign multiple authorization objects, for example, RSBPC_CTR and RSBPC_JNL to the role in the role definition, with specified values in the corresponding authorization fields.
4. Assign the role to specific users in this transaction. You can also choose to append the role to a user profile in transaction SU01.

7.6 Authorization Levels and Their Precedence (Embedded only)

Configuring a Dimension as Authorization Relevant

To configure a dimension as relevant for authorization, follow the steps below:

1. Run transaction RSD1.
2. Enter the dimension's technical name and choose *Maintain*.

3. In the maintenance screen that appears, choose the *Business Explorer* tab and then select *Authorization Relevant*.

Authorization Levels

- SAP BW Analysis Authorization
  Defined centrally in the BW backend system. The data access is controlled independently from other data access tools.
  This type of authorization is defined in transaction `RSECADMIN` and is assigned to a user.
- Environment Authorization
  Extend the BW analysis authorization to an environment in Planning and Consolidation.
- Data Access Profile
  The owner of Planning and Consolidation environment can define a data access profile and assign it to Planning and Consolidation users.

Creating an SAP BW Analysis Authorization

1. Run transaction `RSECADMIN` and create a standard analysis authorization.
2. Assign the authorization to a `PFCG` role and generate a SAP NetWeaver profile with transaction `PFCG`.
3. Run transaction `SU01` and assign the `PFCG` role or the NetWeaver profile to a user.
   For more information, see the SAP BW analysis authorization documentation, available on the SAP Help Portal.

Creating an Environment Authorization

1. Create a standard SAP BW analysis authorization.
2. To assign the analysis authorization to a Planning and Consolidation environment, run transaction `RSECENVI`.
3. Enter the environment name.
4. On the next screen, choose the required BW analysis authorizations.

Creating a Data Access Profile

1. Go to the *Administration* page and under the *Security* section, choose *Data Access Profile*.
2. On the screen that appears, choose *New*.
3. Enter the ID and description of the new data access profile.
4. Select the required model from the list.
5. For each authorization relevant dimension, select the required members and set their access rights.
   Important: Be sure to read the note below.
6. Go to the *Users* or *Teams* tab to assign the new data access profile to users that are assigned to the current environment or teams that have corresponding users assigned to it.

> **i Note**
>
> You can group several members by hierarchy and access rights. To do that, select the required members and choose *Group*.
>
> You can split a member to separate lines for easier access rights maintenance. To do that, select the required member and choose *Split*.
>
> In step 5 above, if the members you select come from a hierarchy, you can further define the selection range according to the relationship and level of the selected member in the hierarchy. However, if you choose *All Members* or *Aggregation*, or you select members from a flat view, you will not be able to further define such a selection range. For instructions on how to use *Relationship* and *Level* to define a certain

selection range, review this example in which you select member **China** from a hierarchy level that has been defined as shown below:

Level 0	Level 1	Level 2	Level 3
Asia	China	Shanghai	A1
			A2
		Beijing	B1
			B2
EUR	FR	PARIS	E1
			E2

After selecting China in this example, you then choose one of the five relationships and define levels of how deep in the hierarchy you want the access right to take effect:

- If you choose *Only Selected Nodes*, the access right affects only China, which is the exact member you select.
- If you choose *Subtree Below Nodes*, the access right affects China and all of its descendants.
- If you choose *Subtree Below Nodes to Level (Static to Hierarchy)* and set the level value to **2**, this defines to which level the selection range expands, starting from the root level, also known as level 0. In this case, the affected members start from China and end at the level 2 members Shanghai and Beijing.
- If you select *Subtree Below Nodes to Level (Relative to Node)* and set the level value as **2**, this defines to which level the selection range expands, starting from the selected member. In this case, the affected members are China and all members from the next two levels, which are Shanghai and Beijing in level 2 and A1, A2, B1, B2 in level 3.
- If you choose *Complete Hierarchy*, the access right affects all the members in the current hierarchy.

Example

In the following example there are two dimensions - Customer and Country. The possible values for the Customer dimension are 1, 2, 3 and 4, and the possible values for the Country dimension are DE and FR. The access rights for these dimensions are defined as follows:

Analysis Authorizations

Dimension	Value
Customer	1, 2, 3
Country	DE

Dimension	Value
Customer	4
Country	FR

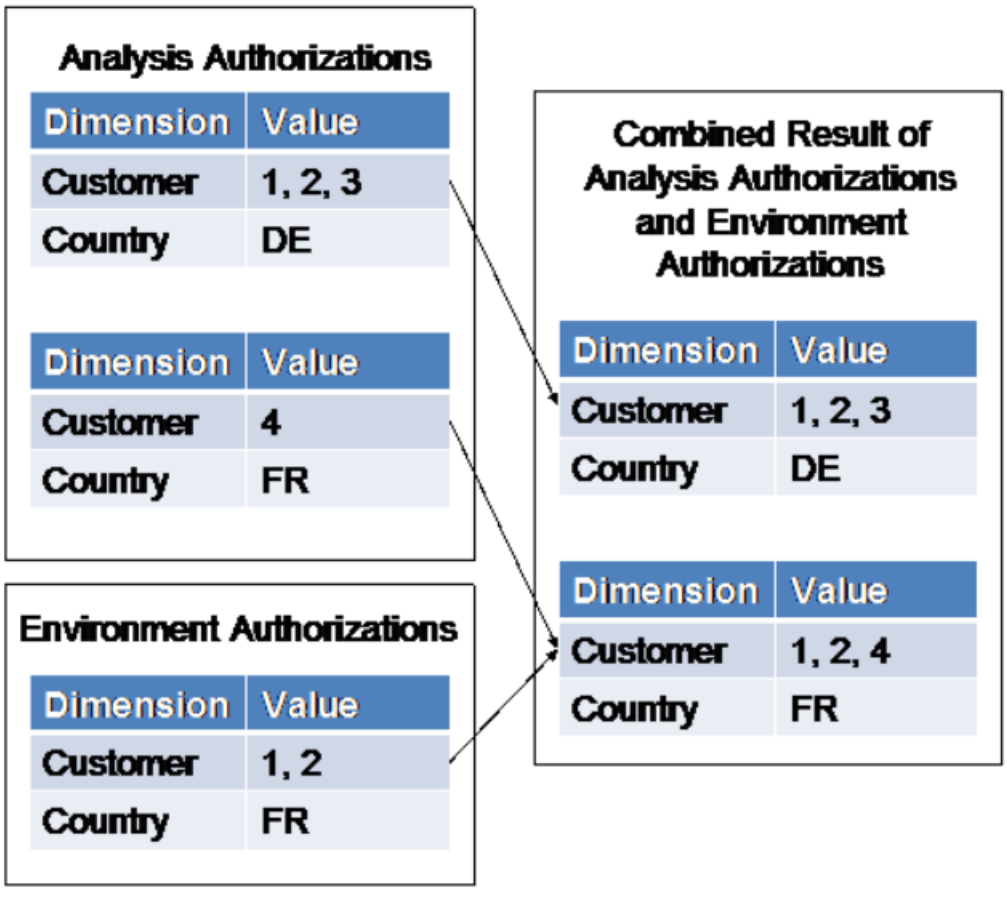
Environment Authorizations

Dimension	Value
Customer	1, 2
Country	FR

Data Access Profile

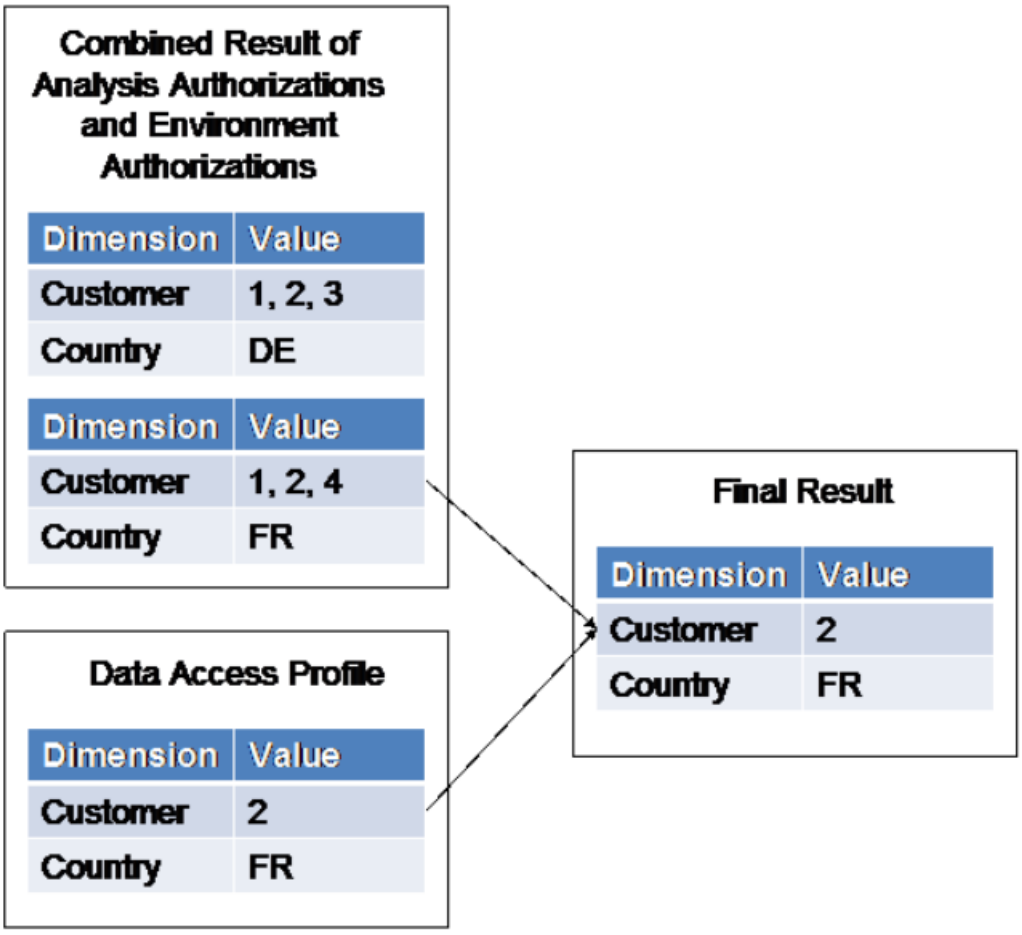
Dimension	Value
Customer	2
Country	FR

When the analysis authorizations and the environment authorizations are combined, customers 1, 2 and 4 all gain authorizations for country FR. The authorizations for country DE are not changed:



After the data access profile is added to the combined result of the previous step, only customer 2 has authorizations for country FR because that is the only customer that appears in both the combined result and the data access profile.

The data access profile does not define any permissions for country DE. There is no intersection between the combined result of the previous levels and the data access profile. Because of that the permissions for country DE are entirely excluded from the final combination of authorizations.



8 Network and Communication Security

8.1 Introduction

Your network infrastructure is important in protecting your system. Your network needs to support the communication necessary for your business and your 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, 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 Planning and Consolidation 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 Planning and Consolidation. Details that specifically apply to Planning and Consolidation are described in the following topics:

- Communication Channel Security
  This topic describes the communication paths and protocols used by the application.
- Network Security
  This topic describes the recommended network topology for the application. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection.

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

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability Technologies*

8.2 Communication Channel Security

Use

The following table shows the communication channels used by the application adapter, the protocol used for the connection, and the type of data transferred:

Communication Channel	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front-end client using a web browser to application server	HTTP, HTTPS, SSL (REST communication is used)	Example: All application data	UI configuration

HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

For more information about transport layer security, see the SAP NetWeaver Security Guide on SAP Help Portal at http://help.sap.com *SAP NetWeaver*.

Authentication is needed to access the application; access to different content areas is protected using authorization checks based on ABAP Authorization Objects.

> **i** Note
>
> We recommend HTTPS for enhanced security. HTTPS is required to secure communication between the client and the NetWeaver application server.
>
> The RFC destination is used for after-import transactions for transports on the ABAP side, and must be configured exclusively for the Planning and Consolidation application. For more information on creating the RFC destination, see the **Configuring the ABAP Component** section of the *Installation Guide*.
>
> For information about application ports, see the **Server Options** section in the *Administrator's Guide* or the *Installation Guide*.

> **→** Recommendation
>
> - You should configure the browser to clean the cache when the browser is closed. For example, in Internet Explorer, select the option *Empty Temporary Internet Files folder when browser is closed* in the Advanced tab.
> - Sensitive data – for example, user identifiers and names of the users – might be exposed through temporary file storage in Internet browsers, where the temporary storage is not on a secure file system. We recommend that you apply secure settings to Internet browsers. Ensure that a secure file system is used for the temporary storage, that is, NTFS rather than FAT on a Windows operating system.

The following table shows the communication channels used by event and notification, the protocol used for the connection and the type of data transferred:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Adobe Flex-based UI in application framework (in client browser) communicates with application server hosting event and notification	HTTP (REST over HTTP)	User interaction data	N/A
Java application (server) communicates with application server hosting event and notification	HTTP (REST over HTTP)	System interaction data	N/A
ABAP application server sends messages to e-mail server	SMTP	E-mail notifications to users	N/A

The following table shows the communication channels used by context, the protocol used for the connection and the type of data transferred:

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Adobe Flex-based UI in application framework (in client browser) communicates with application server hosting context	HTTP (REST over HTTP)	User interaction data	N/A
Java application (server) communicates with application server hosting context	HTTP (REST over HTTP)	System interaction data	N/A

8.3 Network Security

Use

You can implement the following components of the application in different network segments:

- Front-end client
- NetWeaver application server

We recommend either of the following environments, based on your on your technical requirements.

- All components in one network zone (LAN)
- Client in Internet zone; NetWeaver tier in a different zone

> **i Note**
>
> The NetWeaver tier includes a database server and an optional SAP NetWeaver Business Warehouse Accelerator, therefore we support a NetWeaver application server, and a NetWeaver database and the accelerator in a different network zone.

The application relies on the networking infrastructure provided by SAP NetWeaver. As a result, network security related information explained in the SAP NetWeaver Security Guide also applies to the application. It does not impose any special requirements on the setup of the network beyond those documented in the SAP NetWeaver Security Guide.

9 Data Storage Security

Use

Data is stored by the application exclusively in the primary database of the SAP NetWeaver Application Server ABAP.

Storage of replicated data is not allowed outside the primary database.

For more information about access control on database and operating system level, see the security-relevant documentation of your database and operating system.

Access to data stored in the database throughout various locations can be secured by configuring access controls according to the guidelines in the Authorizations section.

For guidelines about securing data located in the primary database of SAP NetWeaver Application Server ABAP, see the SAP NetWeaver Security Guide and the documentation of the database product used.

10 Other Security-Relevant Information

Security Management Conflict with SAP Central User Administration

When SAP Central User Administration (CUA) is enabled, the underlying NetWeaver API throws an exception when trying to perform certain security-related actions, for example, assigning a user to a NetWeaver role/profile from Planning and Consolidation.

Since CUA was designed to be the only security administration of NetWeaver when it is enabled, NetWeaver security APIs reject any calls from other parties. To support user management in the web client of Planning and Consolidation, the related call is delegated to the CUA system. Since the synchronization of the SAP NetWeaver roles/profiles between the central CUA system and the child systems is performed periodically through a background job, there are some limitations when managing security through the Planning and Consolidation web client. For more information, see SAP note 1880183.

Virus Scanning

The application performs a virus scan of content (for example, chart templates) when that content enters the application via upload or import.

When uploading a template, the user can upload two types of files:

- SWF File
- XLF File

The upload wizard checks for the file type to make sure that the uploaded files are of types SWF and XLF only. If the check on the file type fails, the wizard prompts the following error message: *Selected file type is not supported*.

For more information about virus scanning, see *SAP Virus Scan Interface* in the SAP NetWeaver documentation on SAP Help Portal at http://help.sap.com *SAP NetWeaver*.

HTTP Caching

> → Recommendation
>
> We recommend using HTTP 1.1 caching compliant proxies for performance reasons.
>
> HTTP 1.0 is supported, but performance is significantly lower.

Preventing Clickjacking in the Web Client

SAP UI5 provides a solution to resolve clickjacking issue in the web client. You must implement the badI `/UI5/BADI_CONFIG_HTTP_HANDLER` method `/UI5/IF_CNFG_HTTP_HNDLR~RESTRICT_IFRAME_USE` to forbid the Business Planning and Consolidation web client from being embedded in one HTML frame. For more detail, see SAP note 2075016.

Dynamic CSRF Token

A security enhancement that supports dynamic CSRF tokens is available in Business Planning and Consolidation 10.1 NW 740 SP10 and release 10.1 NW 750 SP03.

To enable the dynamic CSRF token, you need to create a new parameter called `FORCE_DYNAMIC_CSRF_TOKEN_CHECK` via transaction `SPRO`, a global setting shared by both the standard and embedded configurations of the application.

After enabling the dynamic CSRF token, you need to upgrade the EPM Add-in or AO to the following versions:

- EPM Add-in: Version 10.1 SP25 or above
- AO: Version 2.2 SP02 or above

For more details, refer to SAP note 2307532.

11 Dispensable Functions that Affect Security

Planning and Consolidation uses the following system resources:

- Client tier – File system, system components, operating system
- NetWeaver/ABAP server – System components, operating system

There are no administration tools or installation tools that can be deleted after installation.

Server Installation

For the server installation, all functional modules are necessary and are used at runtime.

An installation contains a default environment named EnvironmentShell. This is the only component you can remove after you complete your own environment development.

> → Recommendation
>
> We recommend that you do not remove EnvironmentShell as it is often used by SAP Active Global Support in troubleshooting customer issues.

12 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with applicable data privacy regulations, it is necessary to consider compliance with industry-specific legislation in different countries.

SAP provides specific features and functions to support compliance with regards to relevant legal requirements, including data protection. SAP does not give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, this information does not give any advice or recommendations regarding additional features that would be required in particular IT environments; decisions related to data protection must be made on a case-by-case basis, under consideration of the given system landscape and the applicable legal requirements.

In the majority of cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion of personal data. SAP does not provide legal advice in any form. Definitions and other terms used in this document are not taken from any given legal source.

> **i Note**
>
> Due to the local nature of BW workspace data, which is owned by single users or user groups rather than centrally, we do not recommend the use of personal data in BW workspace objects, or in other words, BPC local objects.

Related Information

Security Standards [page 56]
Glossary [page 63]

12.1 Security Standards

The following standards apply to SAP Business Planning and Consolidation:

Related Information

Glossary [page 63]

12.1.1 User Consent

SAP Business Planning and Consolidation does not collect any personal data.

If any customer installations collect and process any personal data, SAP assumes that the customer receives consent from data subjects.

12.1.2 Read Access Logging

Read access logging is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy.

Logging of read access to sensitive data can be implemented in several different ways depending on the BPC configuration and type of data.

If you are using a standard configuration of BPC, refer to Logging of Read-access to Master Data (Standard only) [page 57] and Logging of Read-access to Transaction Data (Standard only) [page 58] for more details.

If you are using an embedded configuration of BPC, refer to Logging of Read-access to Master Data and Transaction Data (Embedded only) [page 58] for more details.

12.1.2.1 Logging of Read-access to Master Data (Standard only)

Administrators can check detailed information about who at what time has read master data in Business Planning and Consolidation at the dimension level. To enable such auditing, follow these steps:

1. Enter transaction code `SPRO` and go to *SAP Reference IMG* > *Business Planning and Consolidation* > *Standard* > *Configuration Parameter* > *Set Environment Parameters*.
2. Choose your environment and create a new parameter with the field name *MD_READ_AUDIT*.
3. In the *Value* field, enter the names of the dimensions for which you want to check their read status. If you want to check only some properties of the dimensions, enter the value in the form, such as `Account (ACCTYPE, GROUP, ELIMACC); Entity (CURRENCY)`. If the value field is left empty, no information will be recorded.

After you set up the prerequisites above, you can check master data information in the table *UJU_AUDACTHDR2* and *UJU_AUDACTDET2* via transaction code `se16`.

12.1.2.2 Logging of Read-access to Transaction Data (Standard only)

Administrators can check detailed information about who has read transaction data in Business Planning and Consolidation via the BAdI *UJQ_SHARED_QUERY*.

12.1.2.3 Logging of Read-access to Master Data and Transaction Data (Embedded only)

Prerequisite

As BPC leverages BW/4HANA's logging feature to log read access to master data, we recommend not assigning users the authorization to maintain master data in BPC's master data maintenance page. To set this authorization, go to BW modeling tools and maintain the authorization object *S_RS_IOMAD*. For detailed information, refer to Authorization Objects for Modeling (Embedded only) [page 38].

Activity

In the embedded configuration of BPC, which is the same as that in BW/4HANA, we recommend use LOPD authorization-based logging for logging read access to transaction data. LOPD was developed to achieve compliance with the Spanish data protection law (Ley Orgánica de Protección de Datos de Carácter Personal, known as LOPD). For detailed information, go to Security Guide SAP BW and choose *Data Protection and Privacy* > *Read Access Logging* > *Logging of Transaction Data: LOPD Authorization-Based Logging*.

For logging of master data maintenance in Web Dynpro ABAP, we recommend use Read Access Logging (RAL). For detailed information, go to Security Guide SAP BW and choose *Data Protection and Privacy* > *Read Access Logging* > *SAP NetWeaver Read Access Logging in SAP BW*.

Another approach to logging read access to master data is to first load master data into an InfoProvider via an ETL process, then use LOPD authorization-based logging to generate read access logs in the InfoProvider. After the loading, you need to use standard reporting techiques to read master data from the InfoProvider. For detailed information,go to Security Guide SAP BW and choose *Data Protection and Privacy* > *Log Changes to Personal Data*.

12.1.3 Log Changes to Personal Data

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to be able to track the changes made to this data. If these changes are logged, you can

check which employee made which change and when at any time. It is also possible to analyze errors in this way.

Logging of changes to personal data can be implemented in several ways depending on the BPC configuration and type of data.

If you are using a standard configuration of BPC, refer to Logging of Changes to Master Data (Standard only) [page 59] and Logging of Changes to Transaction Data [page 60] for detailed information.

If you are using an embedded configuration of BPC, refer to Logging of Changes to Master Data (Embedded only) [page 59] and Logging of Changes to Transaction Data [page 60].

12.1.3.1 Logging of Changes to Master Data (Standard only)

Administrators can check detailed information about who has added or updated master data and what master data has been modified in the BPC web client, under the condition that activity auditing on administration tasks has been enabled.

To enable auditing for Administration tasks, choose *Administration* and under the *Audit* section choose *Administration Activity* > *Enable Auditing of Administration Activity*. Once the system records an activity, you can run a report that shows activity based on specified criteria. For more information, see *Reporting on Administration Activity* in the application help.

12.1.3.2 Logging the Back-up and Restore of Environment (Standard only)

Administrators can view who backed up or restored an environment and at what time using UJBR in the table *UJU_AUDACTHDR2* and *UJU_AUDACTDET2*, as long as the *Audit Data Changes* option has been turned on. For detailed information, refer to *Data Auditing* in the application help.

12.1.3.3 Logging of Changes to Master Data (Embedded only)

Prerequisite

As BPC leverages BW/4HANA's logging feature to log read access to master data, we recommend not assigning users the authorization to maintain master data in BPC's master data maintenance page. To set this authorization, go to BW modeling tools and maintain the authorization object *S_RS_IOMAD*. For detailed information, refer to Authorization Objects for Modeling (Embedded only) [page 38].

Activity

In the embedded configuration of BPC, for logging of changes to master data, we recommend first loading master data into an InfoProvider via an ETL process, then use standard planning techniques to maintain the master data in the InfoProvider where the auditing feature can be leveraged to log any changes. For detailed information, go to Security Guide SAP BW and choose *Data Protection and Privacy* > *Log Changes to Personal Data* and refer to the section *Master Data*.

12.1.3.4 Logging of Changes to Transaction Data

Administrators can view who has added or updated transaction data and what transaction data has been modified in the BPC web client once data auditing on administration tasks has been enabled. See *Data Auditing* in the application help.

To enable auditing for transaction data, choose *Administration* and under the *Audit* section choose *Data Changes*. Once the system records an activity, you can run a report that shows activity based on specified criteria. For more information, see *Reporting on Data Changes* in the application help.

12.1.4 Logging of Read-access and Changes to Documents and Files (Standard only)

Administrators can view who has read, uploaded, downloaded, and updated BPC documents, script logic files, and other files uploaded via AO add-in and Data Manager after enabling the IMG environment parameter *UJFS_AUDIT*:

1. Enter transaction code `SPRO` and go to *SAP Reference IMG* > *Business Planning and Consolidation* > *Standard* > *Configuration Parameter* > *Set Environment Parameters*.
2. Choose your environment and create a new parameter with the field name *UJFS_AUDIT*.
3. In the *Value* field, enter value **x**.

After you set up the prerequisites above, you can check transaction data related information in the tables *UJU_AUDACTHDR2* and *UJU_AUDACTDET2*.

12.1.5 Archiving Data Recorded in Audit Tables (Standard only)

To archive some of the data audited in tables *UJU_AUDACTHDR2* and *UJU_AUDACTDET2*, run the Data Manager package */CPMB/ARCHIVE_ACTIVITY*. After doing so, this data is archived into the two archiving tables *UJU_AUDACTHDR2_A* and *UJU_AUDACTDET2_A*.

12.1.6 Deletion of Personal Data

Simplified Blocking and Deletion

In addition to compliance with the general data protection regulation, it is necessary to consider compliance with industry-specific legislation in different countries. A typical potential scenario in certain countries is that personal data shall be deleted after the specified, explicit, and legitimate purpose for the processing of personal data has ended, but only as long as no other retention periods are defined in legislation, for example, retention periods for financial documents. Legal requirements in certain scenarios or countries also often require blocking of data in cases where the specified, explicit, and legitimate purposes for the processing of this data has ended, but the data has to be retained in the database due to other legally defined retention periods. In some scenarios, personal data also includes referenced data. Therefore, the challenge for deletion and blocking is to first handle referenced data and finally other data, such as business partner data.

Deletion of Personal Data

The handling of personal data is subject to applicable laws related to the deletion of such data at the end of purpose (EoP). If there is no longer a legitimate purpose that requires the use of personal data, it must be deleted. When deleting data in a data set, all referenced objects related to that data set must be deleted as well. It is also necessary to consider industry-specific legislation in different countries in addition to general data protection laws. After the expiration of the longest retention period, the data must be deleted.

12.1.6.1 Deleting Transaction Data

To delete transaction data in an InfoProvider, use selective deletion of records from the active table. For detailed information, go to Security Guide SAP BW and choose *Data Protection and Privacy* > *Deletion of Personal Data* > *Deleting Transaction Data*.

12.1.6.2 Removing Personal Data from Master Data

Depending on the data model and user's preference, generally clearing personal or sensitive attributes might be sufficient to anonymize the data. The key of the record will persist and all InfoProviders using the InfoObjects will still contain the transaction data referring to this master data record.

If clearing attributes is not sufficient and a master data key must be removed from the system, all usages of that key must be found and the respective records have to be deleted using selective physical deletion.

In a standard configuration of BPC, users with proper master data maintenance authorization can delete personal data in either of these two ways:

- In the BPC web client, go to the master data maintenance page, then select and delete the master data you no longer needed. Note that you need to clear all transaction data related to that master data before deleting them.
- Go to BW modeling tools and delete the data. For detailed information, refer to Security Guide SAP BW and choose *Data Protection and Privacy* > *Deletion of Personal Data* > *Removing Personal Data from Master Data*.

In an embedded configuration of BPC, you can follow the steps described in the chapter *Data Protection and Privacy* > *Deletion of Personal Data* > *Removing Personal Data from Master Data* of Security Guide SAP BW.

12.1.6.3 Deleting Archived Data

In a standard configuration of BPC, if you want to permanently delete archived data saved in the archiving tables, you can execute the program *UJU_DELETE_AUDIT_DATA_2* in BW backend and choose a time range for which you want to delete data. The data in the selection range will be permanently deleted from table `UJU_AUDACTHDR_A`, `UJU_AUDACTDET_A`, `UJU_AUDACTHDR2_A`, and `UJU_AUDACTDET2_A`.

In an embedded configuration of BPC, if you want to permanently delete archived data, refer to the steps mentioned in the chapter *Data Protection and Privacy* > *Deletion of Personal Data* > *Deleting Archived Data* of Security Guide SAP BW.

12.1.7 Information Report

Each person has the right to obtain confirmation as to whether or not personal data concerning himself or herself is being processed.

In BPC, depending on the type of BW object found, you can use the following functions to show the detailed data of the dependent object:

- Transaction data: BW Reporting Preview for the InfoProvider in the BW modeling tools or SAP GUI transaction `LISTCUBE`
- Master data: Master data maintenance
- Hierarchy data: Hierarchy maintenance

For detailed information, refer to Security Guide SAP BW and choose *Data Protection and Privacy* > *Information Report*.

12.2 Glossary

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.
Deletion	The irreversible destruction of **personal data**.
Retention period	The period of time between the end of purpose (EoP) for a data set and when this data set is deleted subject to applicable laws. It is a combination of the residence period and the blocking period.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can be accessed only by users with special authorization (for example, tax auditors).
Sensitive personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data, data concerning health or sex life or sexual orientation • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts

Term	Definition
Residence period	The period of time after the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Where-used check (WUC)	A process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP