Deloitte.

8. Authorisation Challenge

Exploring New Authorisation Objects in SAP S/4HANA

2026

Too much of a good thing.

Authorisation objects in SAP are essential components of the security framework. They ensure users have appropriate access to system resources and functions. They help maintain data integrity by preventing users from changing data beyond their responsibilities. Authorisation objects also ensure data confidentiality by restricting display rights.

Depending on the installed components and business functions, the number of authorisation objects in an SAP S/4HANA system may vary. On average, there are approximately 10,000 authorisation objects in a system. Even an authorisation administrator with 30 years' experience cannot know them all. However, certain authorisation topics in SAP S/4HANA are important in almost every implementation project. Consequently, authorisation consultants tend to have deeper knowledge of the behaviour and significance of specific authorisations.

This article describes a few examples of new authorisation objects in SAP S/4HANA.

Authorisation Objects for Managing Business Partners

The Business Partner functionality replaces the previous customer and supplier master data management in ECC and is now handled centrally through the Business Partner transaction (BP). Permissions in Business Partner management are more tightly controlled by authorisation objects specifically tailored to Business Partner functionality. This allows granular control over who can create, modify, display, or delete specific data in the Business Partner master data.

In SAP S/4HANA, new authorisation objects are introduced not as replacements for the legacy objects but as additional layers on top. A clear example of this is Business Partner authorisations: SAP S/4HANA introduces several new authorisation objects specifically for managing Business Partners. However, the traditional authorisation objects used for customer and vendor master data in SAP ECC remain valid and are still checked by the system.

As a result, granting access to create or modify customers and vendors in SAP S/4HANA requires maintenance of many more authorisation objects than in SAP ECC. The new objects govern access to various aspects of Business Partner data, including roles, attributes, field groups, and relationship categories.

Figure 1 shows some of the key authorisation objects for managing Business Partners.

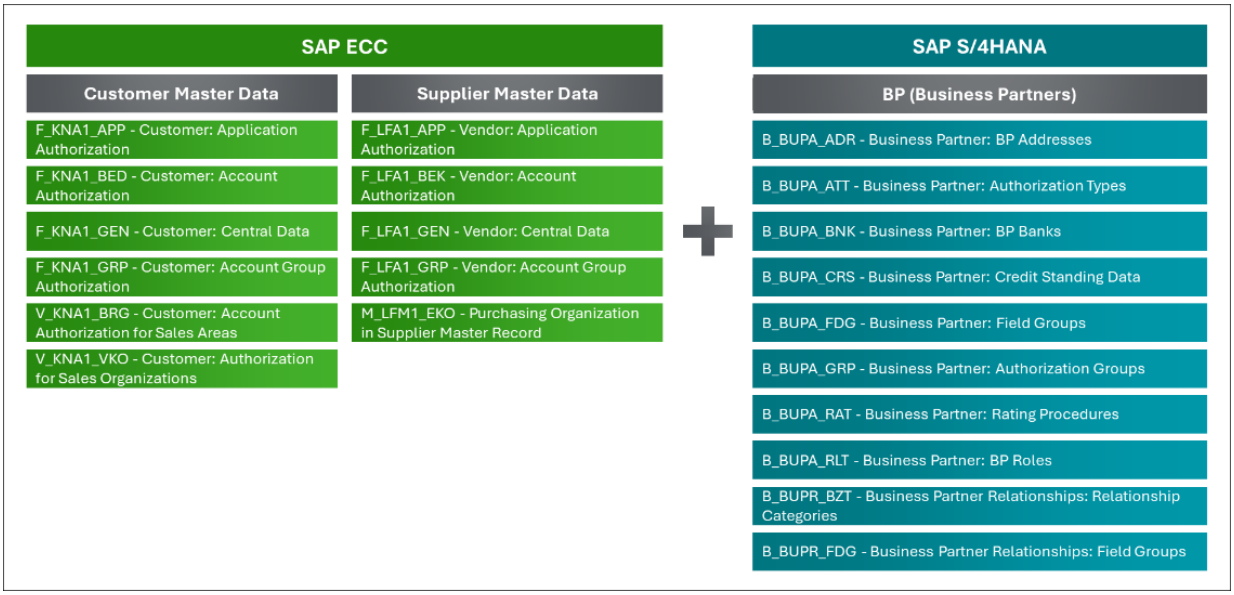


Figure 1: Key Authorisation Objects for Business Partner Maintenance

Nevertheless, in practice, the SAP standard authorisation objects for managing Business Partners often do not fully meet customers' requirements. In a few recent implementations, at least one custom authorisation object for the BP application was implemented.

New Authorisation Objects for SAP Fiori Launchpad

In SAP S/4HANA, when using the SAP Fiori Launchpad, new authorisation objects are introduced. These objects control access to various Fiori components, including tiles, target mappings, and OData services.

To launch the Fiori Launchpad directly from SAP GUI, users require transaction ***/UI2/FLP***, which in turn requires the authorisation object ***S_SERVICE*** – Check at Start of External Services. ***S_SERVICE*** is also required to start and use any UI2 Fiori app.

Values for ***S_SERVICE*** are automatically added to PFCG roles for the Fiori apps in the catalogs assigned to the role. However, some ***S_SERVICE*** values may still be missing. Authorisation administrators should add any missing services to the role menu as ***Authorisation Defaults***. The corresponding values in ***S_SERVICE*** will then be populated automatically. Typically, two services are required for a single UI2 Fiori app – one for the frontend (18 SAP Gateway: Service Groups Metadata) and one for the backend (19 SAP Gateway: Business Suite Enablement — Service).

There are also new authorisation objects that allow administrators to maintain spaces and pages:

- ***/UI2/UIPC*** - Fiori Launchpad Page: Customising
- ***/UI2/UISC*** – Fiori Launchpad Space: Customising

These objects are normally added to administrator roles (for example, authorisation administrators) without restrictions. However, maintenance of spaces and pages can be delegated to the owning departments using naming conventions and wildcards.

For example, a key user in the Finance department could be granted the following authorisation object variants:

- ***/UI2/UIPC*** - Fiori Launchpad Page: Customising
  - ***/UI2/PG_ID*** = ZFI*
  - ***ACTVT*** = 01, 02, 03, 06
- ***/UI2/UISC*** – Fiori Launchpad Space: Customising
  - ***/UI2/SP_ID*** = ZFI*
  - ***ACTVT*** = 01, 02, 03, 06

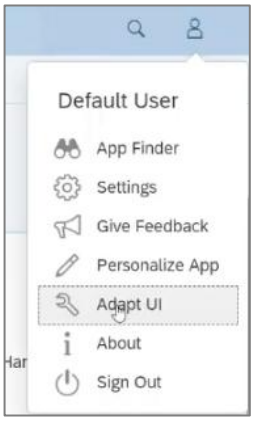
There are also cases where the behaviour of the Fiori Launchpad may be mistaken for missing or excessive authorisations; however, authorisation objects and their values are not the cause. Two common examples:

- Apparent "missing authorisation" for adapting the UI is resolved by assigning the standard catalog ***/UIF/SAP_RTA_PLUGIN***.
- For end users, the ability to change Fiori Launchpad pages is governed by Launchpad parameters and settings rather than the aforementioned authorisation objects, which should only be assigned to system administrators.

How to Grant Authorisation to Adapt UI in SAP FIORI

The ***Adapt UI*** function allows users to personalise and customise the user interface of SAP Fiori applications to better suit their needs. This functionality is part of the SAP Fiori Launchpad and enables enhancements to the user experience without requiring extensive development. To access this function, users require the catalog ***/UIF/SAP_RTA_PLUGIN***.

Once the Fiori application is started, the Adapt UI option appears in the top-right corner under ***User Settings***, as shown in the screenshot below.



Users can then use the graphical interface to make the desired changes to the layout, fields, and sections.

This use case is an example of how authorisations in SAP are managed through menu objects rather than authorisation objects.

How to Remove the Possibility for End Users to Change Launchpad Pages

In many projects, once the roles, spaces, pages, and sections are defined and implemented, functional consultants ask how to prevent users from changing the Fiori Launchpad elements delivered with PFCG roles. They want to avoid situations where, during training, users cannot find Fiori tiles on the Launchpad because they were accidentally removed.

The ability to edit predefined Launchpad pages and sections is controlled by the Launchpad parameters ***HOMEPAGE_PERSONALIZATION*** and ***HOMEPAGE_PERSONALIZATION_HIDEGROUPS*** in transaction ***/UI2/FLP_CUS_CONF*** – Launchpad Customer Settings (see screenshot below).

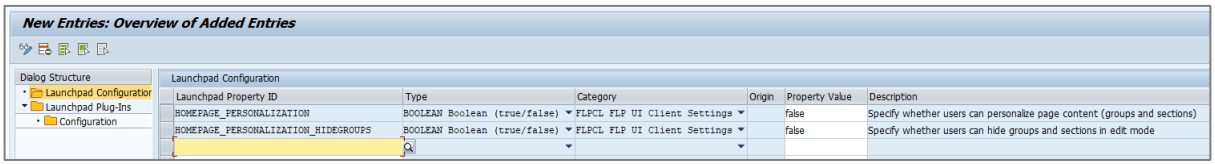
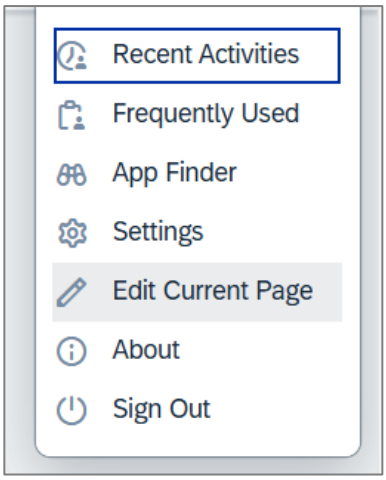


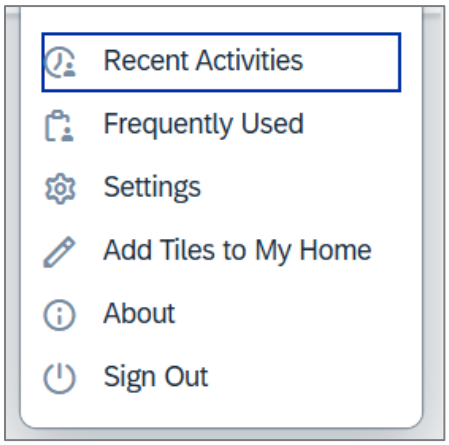
Figure 2: Transaction /UI2/FLP_CUS_CONF - Launchpad Customer Settings

If you do not maintain these parameters, or if you set them to ***true***, users will see an ***Edit Current Page*** button in ***User Settings***. If the parameters are set to ***false***, this button will not be displayed. See the table below.

HOMEPAGE_PERSONALIZATION = true ***HOMEPAGE_PERSONALIZATION = false***

HOMEPAGE_PERSONALIZATION_HIDEGROUPS = true ***HOMEPAGE_PERSONALIZATION_HIDEGROUPS = false***





When these parameters are set to ***false***, note that the ***App Finder*** button will also disappear, and the change applies to all users, not just end users. Therefore, it is recommended to enable Fiori Launchpad personalisation in SAP systems that are not used by end users (e.g., the development system). Users will still be able to find all Fiori apps assigned to them via Search and the ***All My Apps*** menu. They will also be able to maintain their start page, ***My Home***.

How Deloitte Can Help

SAP S/4HANA introduces new authorisation objects that enhance application security and management. These objects augment rather than replace traditional ones, adding layers of control and requiring maintenance of far more authorisation objects than in SAP ECC. By leveraging these new authorisation objects, organisations can achieve granular control over sensitive data, safeguard critical information, and ensure that only authorised personnel can perform specific actions.

Deloitte consultants can help you adapt your security framework to the changes introduced by SAP S/4HANA, so your business can continue to operate securely in the digital economy and fully benefit from S/4HANA's increased agility, efficiency, and innovation.

Deloitte.