Deloitte.

5. Authorisation Challenge

SAP_ALL Is Too Much, and Yet… It’s Not Enough

2026

An ounce of prevention is worth a pound of cure.

In the past, assigning the SAP_ALL profile to project team members in sandbox or test systems allowed them to work freely without encountering authorisation issues. However, in SAP S/4HANA, SAP_ALL only grants backend access; it does not include the necessary permissions to launch or navigate the Fiori Launchpad. To enable full access, additional roles with Fiori-specific authorisations must be assigned, along with a basic end-user role that allows users to start the Fiori Launchpad.

We strongly recommend never assigning SAP_ALL, not even in a sandbox environment. Instead, create broad-access functional roles that enable functional teams to explore all business functions, while excluding access to critical areas such as User and Role Administration, Basis, Security Configuration, Transport Management, and similar functions. Let's refer to this as the 'restricted SAP_ALL profile'.

Consider the following scenario: An organisation has just started an SAP S/4HANA project and has set up a sandbox system, either on-premise or in a private cloud. The Authorisation Administrator is tasked with enabling the project team to start working as soon as possible. In addition to assigning the restricted SAP_ALL profile, the following steps must be executed:

1. Assign the Role for SAP Fiori Launchpad

SAP delivers the standard role SAP_FLP_USER, which is copied during the Fiori Rapid Activation process (see SAP note 2902673), resulting in the creation of role Z_FLP_USER. This role includes the necessary OData services to launch the Fiori Launchpad.

2. Assign Roles for Fiori Applications

In the sandbox system, you may assign SAP standard roles. SAP provides approximately 600 standard business roles, which can be found in the SUIM transaction by searching for roles that begin with SAP_BR. About half of these are country-specific versions, which can be filtered out. The remaining roles should be copied using the Z* naming convention. The corresponding Fiori apps within these roles must then be activated using the task list *SAP_FIORI_CONTENT_ACTIVATION* in transaction *STC01*.

When assigning roles to the project team, only the necessary ones should be used. The more roles – and consequently, Launchpad spaces – a user has, the longer it takes for their Fiori Launchpad to load upon login.

SAP does not recommend activating all standard business roles in the production environment. The more ICF nodes are active, the more vulnerable the system becomes to external attacks. Furthermore, activating unnecessary services can degrade system performance. Therefore, once project activities begin in the development system, only the Fiori apps within the implementation project's scope should be activated. Access to the transaction(s) used to activate ICF nodes must be restricted to SAP Authorisation Administrators and/or SAP Basis Administrators.

The need for Fiori authorisations in addition to the restricted SAP_ALL profile highlights the importance of involving SAP authorisation experts early in the S/4HANA project lifecycle. Their expertise ensures that the project team can operate effectively in sandbox and development environments while also adhering to SAP's security recommendations when activating Fiori applications.

And remember, even in sandbox and development environments, using SAP_ALL is not recommended. Instead, create broader roles that include the necessary Fiori authorisations for functional teams to work in test systems.

How Deloitte Can Help

If your S/4HANA project requires expertise in Fiori authorisations, or if your internal authorisation team lacks the capacity to deliver on time, you can always reach out to the Deloitte SAP Security Team. With extensive experience from numerous S/4HANA implementations, we provide the consultation and support you need.

Deloitte.