Telephone: 01905 62 11 08
Email: info@tangotec.co.uk

Strengthening SAP Security: Using SU24 and SU25

Author: Andy Hartley

Tango Technologies Ltd (TangoTec)

Executive Summary

SAP systems underpin the most critical business processes, and their security cannot be left to chance. Two transactions, SU24 and SU25, are often overlooked but are central to maintaining secure, efficient, and compliant authorisation structures. SU24 governs the daily management of authorisation proposals, while SU25 ensures those proposals remain aligned with SAP standards after upgrades. When used together, they provide a framework for role redesign, upgrade readiness, and audit-grade compliance. This paper explores their purpose, best practice use, and strategic importance.

The Challenge of SAP Security

The SAP authorisation concept is powerful but inherently complex. Poorly maintained roles frequently result in over-authorisation, where users are granted more access than they require, or in segregation of duties conflicts that expose organisations to fraud risk. Upgrades can compound these issues, as outdated proposals disrupt role consistency and force costly remediation. Too often, SU24 and SU25 are treated as technical utilities rather than strategic levers. In reality, they are cornerstones of secure role design and should be embedded into governance processes.

Telephone: 01905 62 11 08
Email: info@tangotec.co.uk

SU24 – Authorisation Proposal Governance

SU24 is the transaction used to maintain customer authorisation proposals for transactions, programmes, and services. These proposals ensure that role builds begin with the correct objects and values, providing a consistent baseline for security. The customer proposal tables, USOBT_C and USOBX_C, are maintained directly in SU24. By contrast, the SAP-delivered proposals are stored in USOBT and USOBX and maintained in SU22; these represent the baseline delivered by SAP and should not be altered in production systems.

Effective use of SU24 requires discipline. Proposals should be aligned with business processes rather than blindly following SAP defaults. Regular reviews are essential to prevent authorisation creep, where values become overly broad over time. Every change should be documented to provide transparency for audit purposes. Organisations should mandate that SU24 proposals are the only input to role generation, avoiding ad-hoc object insertion in PFCG which undermines consistency. It is important to note that SU24 data is system-local and only relevant in the development system where roles are created. There is no need to transport SU24 table content. The only transportable element in this area is SU21 authorisation objects if new ones are created, because roles transported to production must reference existing objects.

SU25 – Synchronising After Upgrades

SU25 is the transaction used to update customer proposal tables after upgrades or support packs, ensuring they remain aligned with SAP's updated baseline. The process begins with an initial copy of SAP's proposals into the customer tables, which is run once after installation. Subsequent steps allow organisations to adjust proposals after upgrades, review new or changed transactions, and compare old and new proposals to identify differences.

Best practice dictates that SU25 should always be run after upgrades or support packs. However, organisations should not blindly accept SAP's new defaults. Each change must be validated against business requirements and segregation of duties controls. Compliance teams should be involved in reviewing proposals, and thorough testing of roles should be carried out before go-live. In this way, SU25 acts as a synchronisation mechanism, ensuring that proposals evolve with SAP's standards while remaining tailored to the organisation's needs.

Telephone: 01905 62 11 08
Email: info@tangotec.co.uk

SU24 and SU25 Together – A Governance Workflow

SU25 imports SAP's updated proposals into the customer tables, while SU24 is used to refine and maintain those proposals for ongoing role design. Together, they form a closed loop of proposal management. SAP delivers updates, organisations refine them, and roles remain secure and compliant. Strategically, SU25 should be viewed as the reset and update mechanism, while SU24 is the daily governance tool. This combination ensures that authorisation proposals are both current and business-aligned, reducing risk and strengthening compliance.

Case Example: ECC to S/4HANA Migration

One of the most significant challenges facing organisations today is the migration from SAP ECC to S/4HANA. This transition is not simply a technical upgrade; it represents a fundamental shift in the way authorisations are structured, particularly with the introduction of Fiori applications and the replacement or consolidation of many traditional transactions. In this context, SU25 becomes indispensable. It provides the mechanism to update customer proposal tables so that they reflect SAP's new baseline, ensuring that the organisation's security framework is aligned with the changed transaction landscape. Without SU25, organisations risk carrying forward outdated proposals that no longer match the new environment, leading to broken roles and unnecessary remediation effort.

Once SU25 has been executed, SU24 takes centre stage. It is through SU24 that organisations refine the proposals delivered by SU25, tailoring them to their specific business processes and enforcing the principle of least privilege. For example, where SAP's defaults may propose broad activity values, SU24 allows the organisation to narrow these down to the precise authorisations required. This refinement is critical in S/4HANA, where the proliferation of Fiori apps can easily lead to over-authorisation if proposals are not carefully managed.

The benefits of disciplined use of SU24 and SU25 during migration are tangible. The process becomes more streamlined, as proposals are updated and refined in a controlled manner rather than piecemeal. The risk of over-authorisation is reduced, since every role is built from a secure baseline and adjusted only where necessary. Audit sign-off is accelerated, because changes are documented and traceable, providing assurance that the migration has not introduced compliance gaps. Conversely, neglecting SU24 and SU25 can have serious consequences. Organisations may inherit

Telephone: 01905 62 11 08
Email: info@tangotec.co.uk

insecure proposals from ECC, leading to roles that are either too permissive or incomplete. This in turn results in costly remediation projects, delayed go-lives, and heightened audit findings.

In practice, successful migrations treat SU25 as the synchronisation step that brings proposals up to date, and SU24 as the governance layer that ensures those proposals are fit for purpose. Together, they provide a structured approach to authorisation management that not only supports the technical migration but also strengthens the organisation's overall security posture.

Recommendations

Organisations should establish a governance process in which SU24 proposals are reviewed on a regular basis, ideally quarterly. SU25 must be run after every upgrade or support pack to ensure proposals remain synchronised with SAP's standards. SU24 and SU25 governance should be integrated with GRC and segregation of duties checks, and all changes should be documented to provide audit readiness.

Keep in mind that when assigning new objects into SU24 mapping, think hard about default values as if you over specify ACTVT for example as default, you may need in some cases to inactivate object versions as it's a dual display and or maintain transaction (e.g MIGO) and if ACTVT default values are 01,02,03 you would always be giving the transaction as a maintain transaction unless you add a manually added version with just 03. Do in these cases it is better to only add 03 as a default or maybe better still make the proposal status as Yes - Without Values and fill in the relevant ACTVT values as required.

In recent releases you can also utilise SU24 variants, and we will talk about those in another paper.

Conclusion

SU24 and SU25 are more than technical transactions; they are strategic enablers of SAP Security. By embedding them into governance processes, organisations can achieve reduced risk through least-privilege access, upgrade readiness through synchronised proposals, and audit-grade compliance through documented, consistent role design. In a landscape where SAP systems drive global business, disciplined use of SU24 and SU25 is not optional — it is essential.