No. 01

SAP SECURITY

SAP Role Design Handbook

Users, roles and authorizations in SAP S/4HANA, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 01

SAP Role Design Handbook

Users, roles and authorizations in SAP S/4HANA, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

SAP Role Design Handbook

Users, roles and authorizations in SAP S/4HANA, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 SAP security in a nutshell 4
2 Users and user types 7
3 Authorization objects and checks 11

PART II · ROLE DESIGN

4 PFCG roles 16
5 Proposal values with SU24 and SU25 21
6 Organizational levels and derived roles 24
7 A role design method 27
8 Ten role design mistakes 31

PART III · OPERATE AND PROTECT

9 Critical authorizations 35
10 Troubleshooting authorization errors 39
11 Change control for roles 42
12 Monitoring and reviews 45
13 Checklists 48

Glossary 50
Further reading 52

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Every SAP system decides, thousands of times a minute, whether a person may do what they are trying to do. Those decisions come from **users**, **roles** and **authorizations** — the core of SAP security. When they are designed well, people can do their jobs, auditors are satisfied and changes are easy. When they are designed badly, access piles up, tickets never end and risks hide in plain sight.

This handbook teaches SAP authorization and role design from the beginning: how users and authorization checks work, how to build roles in `PFCG`, how to use proposal values and organizational levels, how to design a role catalog that stays clean, and how to protect, troubleshoot, transport and review it.

Who this book is for

- **New SAP security analysts** and anyone moving into SAP security from Basis, functional or audit roles.
- **Functional consultants** who need to explain what access their processes require.
- **Auditors and controls teams** who want to understand what they are testing.

How the book is organized

- **Part I — Foundations** (Chapters 1–3): users, user types and how authorization checks work.
- **Part II — Role design** (Chapters 4–8): PFCG roles, proposal values, organizational levels, a practical design method and the most common design

FREE SAMPLE · ojayo.com

mistakes.

- **Part III — Operate and protect** (Chapters 9–13): critical authorizations, troubleshooting, change control, monitoring and checklists.

Conventions

TIP

Practical advice you can apply straight away.

IN SAP

Transactions, objects and product-specific details.

WATCH OUT

Common mistakes and risks.

Transactions and technical names appear in a monospaced font, like `PFCG` or `S_TABU_DIS`. Diagrams are original. Screens marked **Illustration** are simplified drawings, not SAP software, and their values are examples. People and companies in examples are fictional.

A NOTE ON RELEASES

This book focuses on SAP S/4HANA and the ABAP platform, and most concepts also apply to SAP ECC. Details differ between releases; confirm specifics in SAP's documentation for your system. SAP S/4HANA Cloud Public Edition uses a different, app-based access model, touched on briefly in Chapter 4.

FREE SAMPLE · ojayo.com

PART I

Foundations

Users, user types and the way SAP checks authorizations at runtime — the vocabulary every later chapter builds on.

FREE SAMPLE · ojayo.com

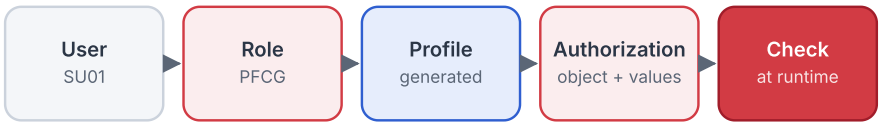
CHAPTER 1

SAP security in a nutshell

SAP security has a small number of building blocks. Learn how they fit together and the rest of the book becomes straightforward.

SAP's authorization concept has been refined over decades, but its core idea is simple: **programs ask questions, and users' authorizations answer them.** Before a program shows a purchase order, posts an invoice or changes a supplier, it asks: *does this user have permission for this kind of object, with these values, for this activity?*

The building blocks



Users get roles; roles generate profiles; profiles hold authorizations; programs check authorizations at runtime.

Figure 1.1 The chain from user to check. Each link is maintained in a different place, and each can be the source of a problem.

- **User** — the account a person (or technical process) uses to log on. Maintained in `SU01`.
- **Role** — a collection of permissions for a task or job, built in `PFCG` (the Profile Generator).
- **Profile** — generated from a role's authorization data; this is what the system actually reads at runtime.

FREE SAMPLE · ojayo.com

- **Authorization** — a concrete permission: an **authorization object** with field values, for example *company code 1000, activity display*.
- **Authorization check** — the moment a program asks the question, using the ABAP statement `AUTHORITY-CHECK`.

When a user logs on, the system loads the authorizations from all of the user's assigned profiles into a **user buffer**. Every check during the session is compared against that buffer.

What “good” looks like

A well-run SAP authorization concept achieves four things:

1. **Least privilege** — people have what their job needs, and no more.
2. **Segregation of duties** — no one person can complete a sensitive process alone.
3. **Maintainability** — roles are understandable, consistent and easy to change.
4. **Accountability** — every access can be traced to an approval, an owner and a person.

These goals pull in different directions. Very fine-grained roles give excellent least privilege but are hard to maintain; very broad roles are easy to maintain but grant too much. Role design is the craft of balancing them.

Who does what

Area	Typical owner
User administration (create, lock, assign)	Security or service desk, through an approved request process
Role design and build	Security team, with functional input
Role ownership and approval	Business process owners
Proposal values (`SU24`) and organizational levels	Security team
Monitoring, reviews and evidence	Security, GRC and internal audit

FREE SAMPLE · ojayo.com

What changed with S/4HANA

SAP S/4HANA keeps the same authorization concept but adds layers:

- **SAP Fiori** apps add launchpad content (catalogs, spaces and pages) and OData service start authorizations to role design.
- **CDS access controls** filter data rows in many modern apps, using the same authorization objects in the background.
- Some classic transactions were **replaced or simplified** (for example, supplier and customer maintenance moved to the business partner).

This book focuses on the authorization foundations that apply everywhere. The *Securing SAP Fiori* volume in this series covers Fiori-specific role design in detail.

TIP

When you start in a new SAP landscape, collect four facts first: the **number of users**, the **number of roles**, the **naming convention** (if any) and the **list of users with critical authorizations**. They tell you more about the state of security than any document.

KEY TAKEAWAYS

- Users get **roles**; roles generate **profiles**; profiles hold **authorizations**; programs run **authorization checks**.
- At logon, authorizations are loaded into the **user buffer**.
- Good design balances **least privilege, SoD, maintainability and accountability**.
- S/4HANA adds **Fiori content, OData services and CDS access controls** on top of the same foundation.

FREE SAMPLE · ojayo.com

CHAPTER 2

Users and user types

Every access decision is made for a user. Getting user administration right — types, groups, validity and locking — is the first line of defense.

Users are maintained with transaction `SU01` (single users) and `SU10` (mass changes). In larger landscapes, users may be managed centrally through **Central User Administration** (CUA) or an identity management system, but the user master in each system still holds the same information.

The user master record

The most important parts of a user master record are:

- **Logon data** — user type, password or SSO settings, validity period, user group for authorization.
- **Address data** — name, department, function, email.
- **Defaults** — date format, decimal notation, logon language.
- **Parameters** — default values for fields in transactions.
- **Roles and profiles** — the access assigned to the user.
- **Groups** — additional grouping for reporting and administration.

The five user types

SAP distinguishes five user types, and choosing the right one is a security decision.

FREE SAMPLE · ojayo.com



Figure 2.1 The five user types and what each is for.

Type	Code	Use	Interactive logon?
Dialog	A	One person, interactive work	Yes
System	B	Background processing and communication within a system (for example internal RFC, workflow)	No
Communication	C	Dialog-free communication for external RFC calls	No
Service	S	A dialog user shared by a larger, anonymous group (for example anonymous web access)	Yes
Reference	L	Not for logon; used to add authorizations to other users	No

Good practice:

- **People get dialog users** — one per person, never shared.
- **Interfaces and jobs get system or communication users** — not dialog users with passwords someone knows.
- **Service users are rare** and must have minimal, carefully reviewed authorizations, because anyone using the service shares them.
- **Reference users** are powerful in a hidden way: authorizations added through a reference user do not appear in the user's own role list. Review them like any other access.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook (you are reading this)
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

SAP Role Design Handbook

Enjoyed it? The full book has 56 pages and 13 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.