

No. 14

SAP HANA

SAP HANA Security

Users, privileges, auditing and encryption in SAP HANA, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 14

SAP HANA Security

Users, privileges, auditing and encryption in SAP HANA, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

SAP HANA Security

Users, privileges, auditing and encryption in SAP HANA, 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 Why SAP HANA security matters 4

2 SAP HANA architecture for security 7

PART II · IDENTITY AND ACCESS

3 Database users 12

4 Authentication and password policy 17

5 Privileges 21

6 Roles 26

7 Analytic privileges and row-level security 30

PART III · PROTECT AND MONITOR

8 Auditing 35

9 Encryption and key management 39

10 Network and operating system hardening 43

11 HANA under SAP applications and in the cloud 46

12 Reviews, monitoring and checklists 49

Glossary 53

Further reading 55

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.

SAP HANA is the in-memory database underneath SAP S/4HANA, SAP BW/4HANA and many other SAP applications — and a platform in its own right for analytics and applications. Everything an SAP system knows ultimately lives in it. Yet HANA security is often treated as "something the Basis team set up once", while all the attention goes to application roles.

That is a gap attackers and auditors both notice. A powerful database user, an active superuser, a missing audit policy or an unencrypted backup can undo the best application authorization concept.

This book explains **SAP HANA security for beginners**: users, authentication, privileges, roles, analytic privileges, auditing, encryption and hardening — with checklists you can use straight away.

Who this book is for

- **SAP security and GRC professionals** who know ABAP authorizations and now need to secure the database layer.
- **Basis and database administrators** responsible for HANA systems.
- **Auditors** reviewing HANA as part of IT general controls.
- **BI and data teams** who give analysts direct database access.

How the book is organized

- **Part I — Foundations** (Chapters 1–2): why HANA security matters, and the architecture you need to understand.

FREE SAMPLE · ojayo.com

- **Part II — Identity and access** (Chapters 3–7): users, authentication and passwords, privileges, roles, and analytic privileges.
- **Part III — Protect and monitor** (Chapters 8–12): auditing, encryption and keys, network and operating system hardening, HANA in ABAP landscapes and in the cloud, and reviews and checklists.

Conventions

TIP

Practical advice you can apply straight away.

IN SAP

Product-specific details, such as SQL statements, parameters and tools.

WATCH OUT

Common mistakes and risks.

SQL and parameter names appear in `code style`. Diagrams are original. Screens marked **Illustration** are simplified drawings, not SAP software, and values in them are examples. People and companies are fictional.

A NOTE ON VERSIONS

This book is written for the **current** generation: **SAP HANA 2.0 SPS08** on premise and **SAP HANA Cloud**. SAP planned SPS08 for Q4 2024 and announced that from SPS08 onward a new support package stack comes every two years with a four-year maintenance period; SAP HANA Cloud follows continuous delivery. Older features that SAP has **deprecated** — XS classic, the classic HANA repository and SAP HANA studio — are mentioned only so you can recognize and retire them. Always confirm details in the SAP HANA Security Guide and SAP Notes for your revision.

FREE SAMPLE · ojayo.com

PART I

Foundations

Why database security matters in SAP landscapes, and the parts of SAP HANA you need to understand before securing it.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why SAP HANA security matters

Application roles protect the front door. The database is the vault behind it. This chapter explains why the vault needs its own locks.

The database holds everything

In an SAP S/4HANA system, the database contains every business document, master record, user record and configuration table. The ABAP application server checks authorizations before it reads or writes data — but anyone who can talk **directly** to the database can bypass those checks entirely.

That is why database security is not a technical detail. It decides whether your application authorization concept can be trusted at all.

Ways around the application

Direct database access can happen through:

- **powerful database users** — for example the built-in superuser, or administrators with broad system privileges;
- **SQL clients** used by analysts, developers or tools;
- **technical users** for interfaces, data loads and replication, whose passwords are stored in many places;
- **operating system access** to the HANA host, its files, traces and backups;
- **backup files** copied elsewhere and restored into another system.

Each path needs its own controls.

FREE SAMPLE · ojayo.com

What goes wrong

Security reviews of HANA systems often find similar issues. SAP's own EarlyWatch Alert security materials list examples such as the HANA user SYSTEM being active and valid, HANA users with critical authorizations like the DATA ADMIN privilege, and an audit log that is not active or is written to an insecure target. Other common findings:

- shared administrator accounts with no personal accountability;
- privileges granted directly to users instead of through roles;
- grantable privileges ("with grant option") spread widely;
- analysts with broad `SELECT` on business schemas;
- weak or never-changed passwords for technical users;
- trace files containing sensitive data left on disk;
- encryption not enabled, or encryption root keys not backed up.

IN SAP

SAP publishes the **SAP HANA Security Guide** and **SAP HANA Security Checklists and Recommendations**. The security guide includes a section on de-activating the SYSTEM user. These documents are the authoritative reference for your version.

Two kinds of HANA use

HANA security depends on **how** the database is used:

- **As an application database** (for example under SAP S/4HANA): business users never log on to HANA; the ABAP server connects with a technical database user. Security focuses on administrators, technical users and the infrastructure.
- **As a data platform** (native HANA applications, analytics, data science): many people and tools log on to HANA directly. Then HANA's own users, roles and **analytic privileges** carry the business authorization concept.

Many landscapes have both. Chapter 2 explains the difference in more detail.

FREE SAMPLE · ojayo.com

Shared responsibility inside your team

HANA security usually involves several teams:

Team	Typical responsibility
Basis / DBA	Installation, users for administration, parameters, backups, patches
Security	Role design, reviews, audit policies, monitoring
Infrastructure	Operating system, network, storage, key management
Data / BI	Data models, analytic privileges, analyst access
Audit / GRC	Independent review of controls

Clear ownership prevents the most common gap: everyone assuming someone else handles the database.

KEY TAKEAWAYS

- The database is the **vault**: direct access can **bypass** application authorizations.
- Paths around the application include **powerful DB users, SQL clients, technical users, OS access and backups**.
- Common findings: **active SYSTEM user, critical privileges, missing audit, no encryption**.
- Security depends on whether HANA is an **application database**, a **data platform**, or both.
- Agree **ownership** across Basis, security, infrastructure, data and audit teams.

FREE SAMPLE · ojayo.com

CHAPTER 2

SAP HANA architecture for security

You cannot secure what you cannot picture. This chapter gives you a security-focused map of an SAP HANA system.

Systems and tenant databases

Current SAP HANA 2.0 systems run in **multitenant** mode: one HANA **system** contains a **system database** and one or more **tenant databases**.

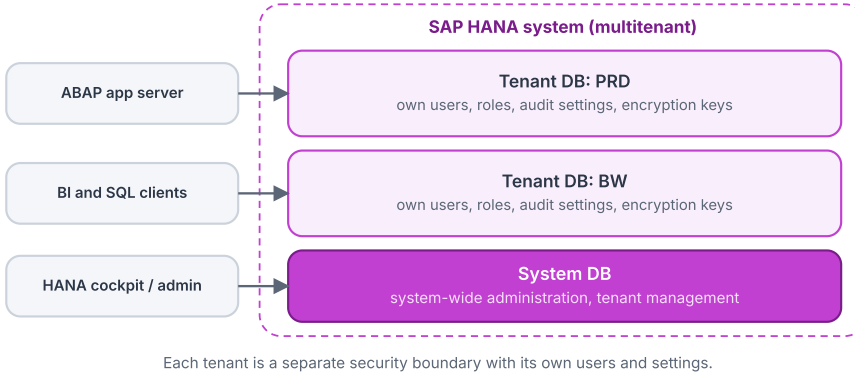


Figure 2.1 A multitenant SAP HANA system. Each tenant has its own users, roles, audit settings and encryption keys; the system database manages the system as a whole.

- The **system database** is used for system-wide administration — for example creating and managing tenants, and system-level configuration.
- Each **tenant database** is an isolated database with its own users, catalog, data and security settings. An application such as SAP S/4HANA uses one tenant.

From a security point of view, this means:

FREE SAMPLE · ojayo.com

- users and roles are **per database** — a user in one tenant does not exist in another;
- **auditing** and **encryption** must be configured for the system database **and** each tenant;
- administrators of the system database have powers over tenants that must be controlled.

Where authorization happens

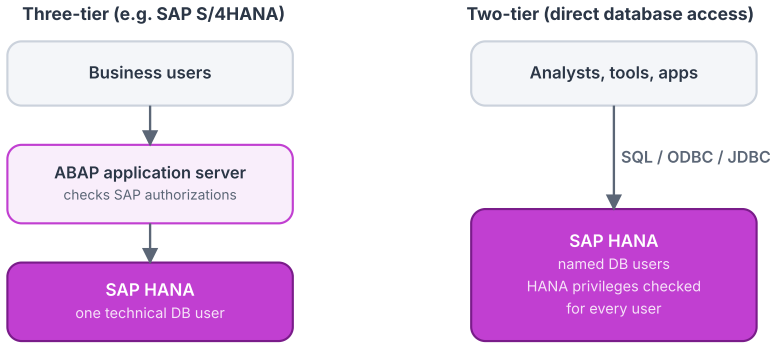


Figure 2.2 In three-tier scenarios, the application server checks business authorizations and connects to HANA with a technical user. In two-tier scenarios, HANA itself checks every user's privileges.

Scenario	Who checks business access	HANA security focus
Three-tier (SAP S/4HANA, BW/4HANA with ABAP)	ABAP authorizations	Administrators, technical users, infrastructure
Two-tier (native HANA apps, SQL analytics)	HANA privileges and analytic privileges	Named users, roles, row-level security

Administration tools

Common tools for HANA administration and security include:

- **SAP HANA cockpit** — the current web-based administration tool, including user, role, password policy and audit management;

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
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 (you are reading this)
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 HANA Security

Enjoyed it? The full book has 60 pages and 12 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.