

No. 43

SAP ANALYTICS CLOUD

SAP Analytics Cloud Security

Users, teams, roles, folders, model data privacy and connections, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 43

SAP Analytics Cloud Security

Users, teams, roles, folders, model data privacy and connections, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

SAP Analytics Cloud Security

Users, teams, roles, folders, model data privacy and connections, 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 What SAP Analytics Cloud is 5
2 The layers of SAC security 7
3 Sign-on and identity providers 9

PART II · USERS AND CONTENT

4 Users and provisioning 12
5 Teams 14
6 Roles 16
7 Files and folders 18
8 Sharing 20

PART III · DATA SECURITY

9 Model data privacy and data roles 23
10 Data access control in dimensions 25
11 Live connections 27
12 Import connections 29
13 Planning security 31
14 SAC content models 33

PART IV · OPERATING SAC

15 Transporting content 35
16 Monitoring and reviews 37
17 Data protection 39
18 Worked example: HR analytics 41

Checklists 43
Glossary 45
Further reading 46

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 Analytics Cloud (SAC) is SAP's cloud solution for business intelligence, planning and predictive analytics. Users build **stories** (dashboards and reports) and **analytic applications** on top of **models**, which get data either live from source systems such as SAP S/4HANA, SAP BW and SAP HANA, or by importing it into SAC. Finance teams also use SAC for **planning**: budgets, forecasts and what-if scenarios.

Analytics tools concentrate data. A single story can show salaries for a whole country or margins for every customer. This book explains, for beginners, **how to secure SAP Analytics Cloud**: sign-on, users and teams, roles, files and folders, sharing, model data privacy, data access control, live and import connections, planning data, content transport, monitoring and a worked example.

Which versions this book covers

- **SAP Analytics Cloud** in its 2025–2026 quarterly releases, including SAC as part of **SAP Business Data Cloud**.
- Live connections to **SAP S/4HANA**, **SAP BW/4HANA** and **SAP HANA**, through **direct**, **tunnel** and **cloud** connection types.
- Data security through **roles with model data privacy** and **data access control in dimensions**.

SAC releases updates every quarter, and menu paths change. This book focuses on concepts and controls; check the SAP Help Portal for your release.

FREE SAMPLE · ojayo.com

Who this book is for

- **SAP security analysts** extending security to analytics.
- **BI and planning administrators**.
- **Model and story owners** in business teams.
- **Auditors and data protection teams**.

How the book is organized

- **Part I — Foundations** (Chapters 1–3): what SAC is, the layers of SAC security, and sign-on.
- **Part II — Users and content** (Chapters 4–8): users and provisioning, teams, roles, files and folders, and sharing.
- **Part III — Data security** (Chapters 9–14): model data privacy, data access control in dimensions, live connections, import connections, planning, and SAC content models.
- **Part IV — Operating SAC** (Chapters 15–18): transporting content, monitoring and reviews, data protection, and a worked example.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN SAP

Product-specific details and names.

WATCH OUT

Common misunderstandings.

FREE SAMPLE · ojayo.com

KEY IDEA

The one thing to remember from a section.

A note on screens and examples

Screens are **simplified illustrations**, not copies of SAP Analytics Cloud screens. Companies, users, teams and models are invented.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what SAP Analytics Cloud is, the layers of its security model, and how users sign on.

FREE SAMPLE · ojayo.com

CHAPTER 1

What SAP Analytics Cloud is

SAC brings data from many systems into stories and plans. Its security must cover features, content and data.

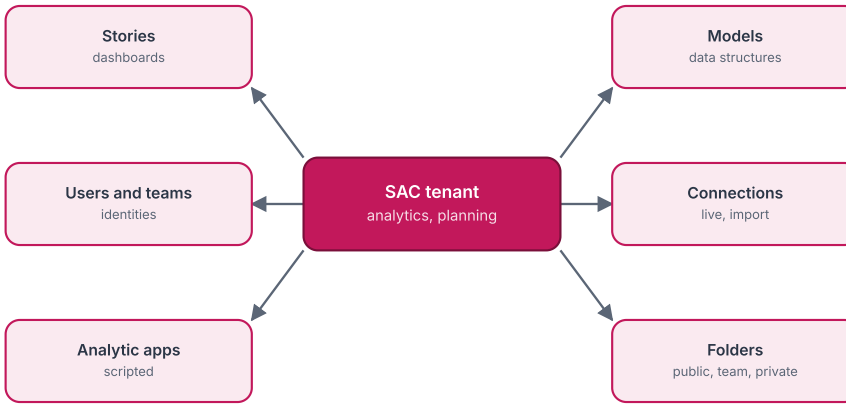


Figure 1.1 The objects that SAC security protects.

Main capabilities

- **Business intelligence**: stories, dashboards and analytic applications.
- **Planning**: budgets and forecasts with versions, data entry and allocations.
- **Predictive**: forecasting and smart insights.

The main objects

- **Stories** and **analytic applications**: what users see.
- **Models**: the structures that define measures, dimensions and data.
- **Connections**: links to source systems, either **live** or **import**.

FREE SAMPLE · ojayo.com

- **Files and folders**: where content is stored and shared.
- **Users, teams and roles**: who may do what.

SAC in the SAP landscape

SAC is a SaaS service hosted by SAP. It connects to on-premise systems through the **SAP BTP Cloud Connector** or directly from the user's browser, and to cloud systems through cloud connections. SAP positions SAC as part of **SAP Business Data Cloud**, together with **SAP Datasphere**, which is covered in its own book in this series.

> **KEY IDEA**
> SAC security has to answer three questions: what can this user do (roles), which content can they open (files and sharing), and which data can they see (data security).

FREE SAMPLE · ojayo.com

CHAPTER 2

The layers of SAC security

SAC security has several layers. A gap in any one of them can expose data.

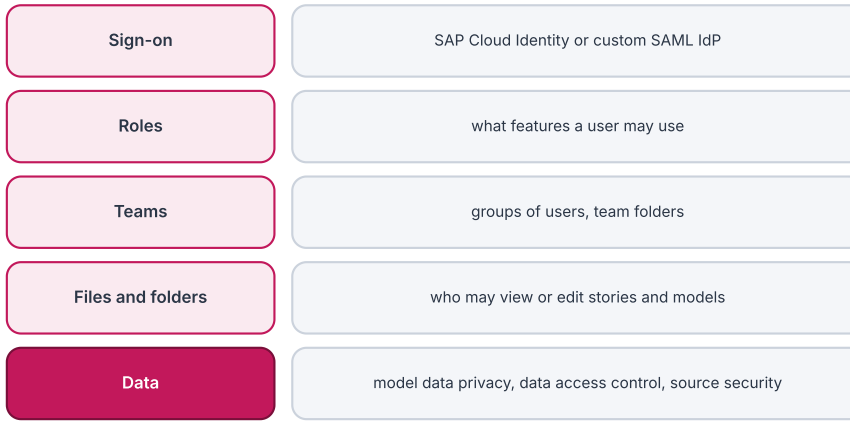


Figure 2.1 The layers of SAP Analytics Cloud security.

Sign-on

Users authenticate through **SAP Cloud Identity Services** (the default) or a **custom SAML identity provider**. Chapter 3 explains the options.

Roles

Roles decide which **features** a user can use: viewing stories, creating models, managing connections, planning, administration. SAC delivers standard roles that can be copied and extended.

FREE SAMPLE · ojayo.com

Teams

Teams group users. Teams can receive roles, and team folders hold content for that team.

Files and folders

Stories, models and other files live in **folders**: private (My Files), team folders and public folders. **Sharing** decides who can view or edit each file or folder.

Data security

Even if a user can open a story, they should see only the **data** they are allowed to. SAC offers **model data privacy** with roles, **data access control in dimensions**, and, for live data, the **source system's own authorizations**.

WATCH OUT

A common mistake is to secure only one layer: for example, putting a salary story in a restricted folder but leaving the model public, so other stories built on it show the same data.

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
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 (you are reading t…
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 Analytics Cloud Security

Enjoyed it? The full book has 51 pages and 18 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.