



Christophe Decamps | Bert Vanstechelman | Chris Walravens

# Securing SAP<sup>®</sup> S/4HANA

- ▶ Effectively secure SAP S/4HANA, Fiori, and Gateway
- ▶ Mobile access and SSO considerations
- ▶ Privileges and roles, authentication, encryption, and monitoring
- ▶ Cross-system authorization concepts and implementation

# Table of Contents

<b>Introduction</b>	<b>7</b>
Acknowledgments	9
<b>1 Securing S/4HANA</b>	<b>11</b>
1.1 Generic steps for back-end roles	11
1.2 ECC authorizations versus S/4HANA authorizations	29
1.3 Conceptual options for SAP roles	32
1.4 Cross-landscape authorizations concept	40
<b>2 Securing Fiori</b>	<b>45</b>
2.1 Deployment options	46
2.2 SAP landscape	50
2.3 Implementing Fiori authentication	52
2.4 Implementing Fiori authorizations	57
2.5 Conceptual considerations	69
<b>3 Securing SAP HANA</b>	<b>73</b>
3.1 Implementing HANA security	73
3.2 Conceptual considerations	89
<b>4 Securing the infrastructure</b>	<b>115</b>
4.1 Securing the application server	117
4.2 Securing data access	130
4.3 Securing SAP Web Dispatcher	143
4.4 Securing the database	146
4.5 Securing the operating system	155
4.6 Securing the network	164
4.7 Conclusion	171

<b>5 Appendix: References</b>	<b>173</b>
5.1 SAP Notes	173
5.2 Articles and other publications	174
<b>A The Authors</b>	<b>176</b>
Christophe Decamps	176
Bert Vanstechelman	177
Chris Walravens	178
About Expertum	179
About SUSAN	180
<b>B Index</b>	<b>185</b>
<b>C Disclaimer</b>	<b>188</b>

## 2 Securing Fiori

**SAP Fiori is a new user experience (UX) for SAP software and applications. It provides a set of applications that are used in regular business functions such as work approvals, financial apps, calculation apps, and various self-service apps.**

The SAP user interface, or SAP GUI as we know it today, was first introduced in 1992 together with the official release of SAP R/3. SAP R/3, the client server edition, was the successor to the SAP R/2 release, the mainframe edition. Although SAP has made several attempts to modernize SAP GUI, an end user from the time it was introduced would still find their way around today. Many transactions and screens have remained the same or changed very little. Since the initial release of SAP GUI, SAP has released several alternative user interfaces such as the SAP Workplace (which was part of the mySAP.com offering), the SAP Enterprise Portal, and the NetWeaver Business Client or NWBC. None were as successful as SAP GUI except, perhaps, for the NetWeaver Business Client. The NetWeaver Business Client is, however, an extension to the SAP GUI. The conclusion of all this is that although many people complained about the old-fashioned look of SAP GUI, they kept using it and will probably continue to do so in the future.

But there is no denying the fact that the user community is changing fast. The SAP users of tomorrow are the youngsters of today, who are used to accessing data from their mobile devices. To them, SAP GUI is a relic from the dark ages. This shift is not limited to youngsters—many end users want data access from any device, from any place, at any time. SAP released SAP Fiori to respond to this demand. SAP Fiori is built using modern design principles you might expect from applications designed for smartphones and tablets. There are already more than 500 role-based Fiori applications such as for HR, Finance, and Business Intelligence. An SAP Fiori application is always limited to a specific task or activity. The design is responsive and deployable on multiple platforms.

There are three types of SAP Fiori applications: transactional apps, fact sheets, and analytical apps.

- ▶ **Transactional or task-based applications:** The transactional SAP Fiori applications are limited to specific tasks such as entering a holiday request or expense note. They give end users fast access to data and represent a simplified view of an existing business process or workflow.
- ▶ **Fact sheets:** Fact sheets have far more capabilities than transactional applications. From a fact sheet, you can drill down into the details. You can even navigate from one fact sheet to another or jump to the related transactional applications. For fact sheets, the underlying database must be SAP HANA. An example of a fact sheet is an application that shows the overview and details of a piece of equipment and its maintenance schedule.
- ▶ **Analytical applications:** Analytical applications build on business intelligence using the capabilities of SAP HANA. They allow you to monitor key performance indicators (KPIs) of your business operations and to react immediately as changes occur. An example is the sales orders application, which immediately shows your sales representative the sales history from his customer, allowing him to take discount decisions immediately.

## 2.1 Deployment options

SAP Fiori apps consist of front-end components, which provide the user interface and the connection to the back end, and back-end components, which provide the data. The front-end components and the back-end components are delivered in separate products and must be installed in a system landscape that is enabled for SAP Fiori. There are multiple deployment options for the SAP Fiori components, each with their respective advantages and disadvantages. SAP Fiori applications are accessed through the SAP NetWeaver Gateway. The gateway consists of two components: *SAP Gateway Foundation (SAP\_GWFND)* and *User Interface Technology (SAP\_UI)*. Both components are add-ons, which from NetWeaver version 7.4, are part of the SAP NetWeaver ABAP Stack. With NetWeaver 7.31, the components had to be deployed separately. This means that any system built on SAP NetWeaver, such as SAP ERP or SAP CRM, can be used to deploy SAP Fiori applications.

The following deployment options exist: *central hub deployment*, the *embedded scenario* and the *cloud edition* (see Figure 2.1).

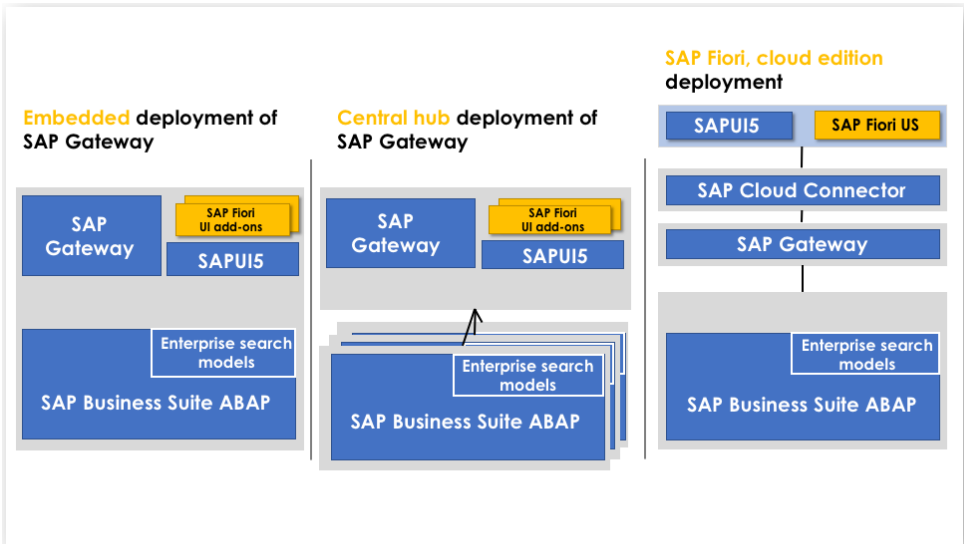


Figure 2.1: SAP Fiori deployment options

### 2.1.1 Central hub deployment

The central hub deployment is the preferred option. Here, SAP NetWeaver Gateway is installed as a separate system. The Fiori applications are deployed here and access the data on the back-end business systems, such as SAP ERP or SAP CRM. Although this option implies an extra system, thus a higher total cost of ownership (TCO), it enables a multi-back-end system scenario while ensuring a consistent look and feel for the different applications. The central hub can be considered a single point of access for all mobile applications. In addition, installing SAP NetWeaver Gateway on a separate system allows you to move the system behind or in front of the firewall depending on your current network topology and security requirements.

### 2.1.2 Embedded scenario

SAP NetWeaver is the basis of all ABAP-based SAP applications, regardless of whether you are talking about SAP ERP, SAP BW, or any of the others. As the gateway is an add-on for SAP NetWeaver, it is available on every ABAP-based business application. This means that it can be activated and that Fiori applications can be deployed on any system. This makes an extra system unnecessary. However, we do not recommend the embedded scenario as, in contrast to the central hub deployment, it results in Fiori applications being installed all over the place—negating the advantage of the single point of access for all mobile applications. The embedded scenario should only be considered during a proof of concept or when the deployment of mobile applications is going to be limited to a single SAP application such as SAP ERP.

### 2.1.3 Cloud edition

The SAP Fiori cloud edition is a ready-to-use infrastructure which can serve as a front end while leaving the back-end systems on premise. The connection to the SAP Fiori Cloud is realized via *SAP Cloud Connector*, which must be installed on premise. The back-end components still have to be installed on the back-end systems.

### 2.1.4 Comparison of the deployment options

Table 2.1 compares the different deployment options. Every deployment option has its respective advantages and disadvantages. The importance of the pros and cons differ in every customer situation.

We strongly recommend the central hub deployment option as it enables a single point of access to your mobile applications for SAP ERP, SAP BW, and many others, while at the same time ensuring the same look and feel. Due to its limitations and dependencies, the embedded scenario should only be considered in a proof-of-concept scenario.

	Central hub deployment	Embedded deployment	Cloud edition
Access	Enables single point of access to multi-back-end scenarios while ensuring a consistent look and feel across back ends	No single point of access for mobile applications	Enables single point of access to multi-back-end scenarios while ensuring a consistent look and feel across back ends
Dependencies	Update dependencies of front-end and back-end components must be considered	One system, dependencies will occur	Update dependencies of front-end and back-end components must be considered
Landscape	Extra SAP landscape and thus a higher TCO	No additional system required	No additional system required
Network	SAP Gateway can be installed in the demilitarized zone (DMZ)	Complicates network topology and security, as many systems may need to be accessible from the outside	SAP Cloud Connector can be installed in the demilitarized zone (DMZ)

*Table 2.1: Comparison of the deployment options*



# B Index

## /

/IWFND/ERROR\_LOG 65  
\_SYS\_BI\_CP\_ALL 100  
\_SYS\_REPO 75

## A

Accumulation of access rights 16  
Authority check 17  
Authorization dependency viewer  
    111  
Authorization objects 11  
Authorization restriction grid (ARG)  
    14  
Authorization statuses 24  
Authorizations concept  
    Composite roles 38  
    Derived roles 36  
Authorizations concept 32  
    Authority check 16  
    Composite roles 15  
    Derived roles 13  
    Profiles 15  
    Single roles 11, 33  
    User buffer 15  
Authorizations procedures  
    Error reporting 28  
    Monitoring 28  
    Role administration 27  
Authorizations procedures  
    User administration 27  
Authorizations testing  
    Composite roles 26  
    Derived roles 25  
    Pilot user approach 26  
    Single roles 25  
Automated provisioning 33

## B

Back-end roles 62, 72

## C

Compliance regulations 33  
Cross-landscape authorizations  
    concept 40

## D

Data access  
    Password policy 141  
    SAP client 130  
    Security Audit Log 137  
    Standard users 138  
    Table logging 134  
DBTABPRT 137  
DDIC 139  
Definer mode 95  
Dependent views 97

## E

EARLYWATCH 139

## F

Fiori 19  
Fiori authentication  
    Basic 52  
    Kerberos 52  
    SAML 54  
    SAP Authenticator 55  
    SAP logon ticket 55  
    X.509 53  
Fiori authentication 52  
Fiori catalogs 57, 70  
Fiori deployment  
    Cloud edition 48

- Embedded scenario 48
- Options compared 48
- Fiori deployment
  - Central hub deployment 47
- Fiori front-end roles 72
- Fiori groups 60, 71
- Fiori launchpad 57
- Front-end roles 61, 69

## G

- Gateway process 120
- Governance model 27
- Grantable to other users and roles 102

## H

- HANA roles 68
  - Catalog roles 87
  - Repository roles 87
- HANA user type
  - Database users 74
  - Internal database users 75
  - Restricted users 74
  - Standard users 74

## I

- Implementation project 17
- Independent views 97
- Internet Connection Framework 126
- Invoker mode 96

## K

- KPI modeler 66
- KPI tiles 67

## L

- Linux 155

## M

- Message server 118

- Monitor authorizations 17
- Monitoring procedures 33
- Multitenant database 107

## N

- Non-organizational fields 13

## O

- Object ownership 91
- Organizational levels 13, 23
- Organizational restrictions 36
- OSS1 170

## P

- PFCG 13, 19, 20, 29, 30, 40, 57, 61
- Privileges 76
  - Analytic privileges 81
  - Application privileges 79
  - Dynamic analytic privileges 85
  - Object privileges 80
  - Package privileges 79
  - SQL analytic privileges 82
  - System privileges 78
  - XML analytic privileges 82
- Profile Generator 19

## R

- Root cause analysis 17
- RSAUDIT\_SYSTEM\_STATUS 140
- RSTBHIST 137
- RSUSR003 140
- Ruleset 17
- Ruleset structure
  - Functions 18
  - Risks 18
  - Rulesets 18
- RZ10 120
- RZ11 120

**S**

S/4HANA 11, 12, 13, 15, 21, 29, 30, 40, 41  
S/4HANA authorizations 11, 29, 40  
S\_RFC 64  
S\_RFCACL 64  
S\_SERVICE 16, 32, 63  
S\_TCODE 16, 17, 18  
S4/HANA 19  
SA38 140  
SAP Access Control 17, 29  
SAP Business Client 12  
SAP GUI 12, 143  
SAP HANA  
    Encryption 147  
    Multitenant 149  
    Revisions 147  
    Secure user store 148  
    System database 150  
    SYSTEM user 151  
SAP HANA client 148  
SAP Host Agent 158  
SAP Identity Management 29  
SAP NetWeaver Gateway 46  
SAP router 167  
    Permission table 168  
    Route string 169  
    saprouttab 169  
SAP Web Dispatcher 51, 143  
SAP\* 139  
SAPCPIC 140  
SAPMMC 164  
SCC4 131, 140  
SCU3 137  
SE13 136  
SE93 16  
SICF 126, 127

SM18 138  
SM19 138  
SM20 138  
SM30 142  
SM51 126  
SMGW 124  
SMICM 126, 128  
SMMS 118  
SQL trace 112  
ST01 65  
ST22 65  
STAUTHTRACE 65  
SU24 20, 21, 25, 32, 37  
SU25 21  
SU53 65  
SYSTEM user 91

**T**

TMSADM 140  
Transaction code 11  
Types of risks  
    Critical access 18  
    Critical permissions 18  
    Segregation of duties (SoD) 18  
Types of risks 18

**U**

User buffer 17  
User-specific trace 112  
USOBT\_C 20  
USOBX\_C 20  
USORG 23  
USR40 142

**W**

Windows 157