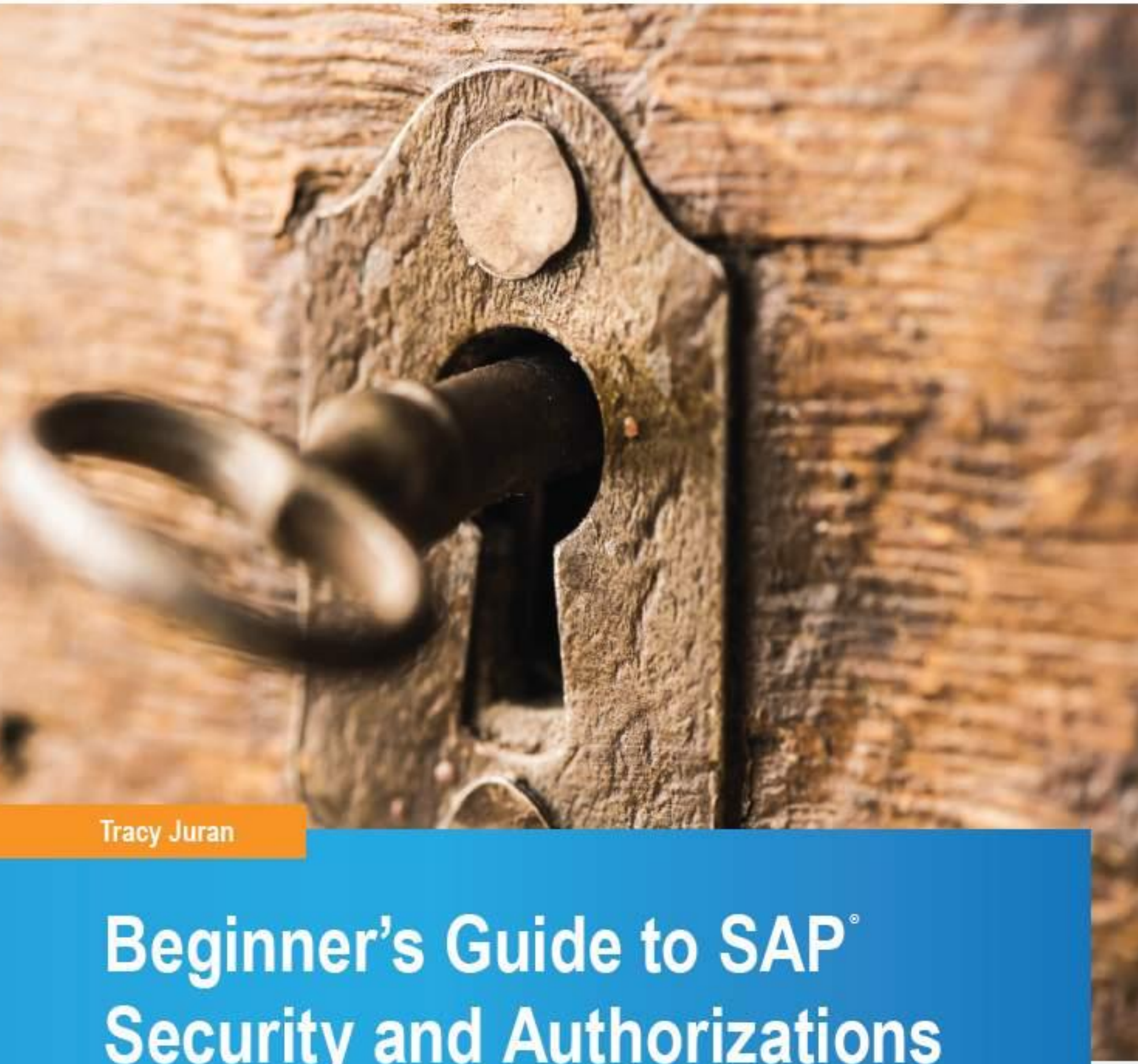
espresso tutorials



Tracy Juran

# Beginner's Guide to SAP® Security and Authorizations

- Basic architecture of SAP Security and Authorizations
- Introduction to GRC Access Control
- Learn how to create users and assign roles
- Troubleshoot common security and authorization pain points

# Table of Contents

**Preface: Introduction to SAP Security and Authorizations concept** **9**

**1 User maintenance overview** **13**

1.1 User master record 14

1.2 User types 24

1.3 User groups 25

1.4 Mass user maintenance (SU10) 27

1.5 Passwords 33

1.6 Central user administration (CUA) 34

**2 Role overview** **35**

2.1 Role types 35

**3 Profile generator and role maintenance overview** **39**

3.1 What is a profile? 39

3.2 What is an authorization? 39

3.3 Profiles and roles 41

**4 Advanced topics for role maintenance** **43**

4.1 Profile generator deep dive 43

4.2 Authorization-object level security 55

4.3 Role type review 61

4.4 Transporting authorizations 68

**5 SAP Security and Authorizations trouble-shooting** **73**

5.1 Reading an SU53 73

5.2 Running a trace (ST01) 75

5.3 Useful SAP Security tables and sensitive authorizations 78

5.4 Maintain authorization object assignment to transaction codes (SU24) 84

5.5 User information system (SUIM) 87

**6 Advanced topics for SAP authorizations 89**

6.1 Upgrading to a new release (SU25) 89

6.2 Introduction to GRC Access Control 91

6.3 Wrap up: Putting a bow on it 94

**7 Acknowledgements 95**

**A The Author 98**

**B Index 99**

**C Disclaimer 101**

# 2 Role overview

**This chapter provides an overview of user roles in SAP and introduces the profile generator transaction (PFCG). A *role* in SAP can be thought of as a person's job in SAP, or a subset of a person's job responsibilities in SAP.**

**Example of a user role in SAP**

For example, if Tracy Levine is a sales clerk at company XYZ, her SAP user roles reflect sales clerk access. Tracy can have one role assigned to her that will be a compilation of all transactions and authorizations required. However, Tracy can also have many roles assigned, which in totality will provide her the permissions necessary to complete her job tasks.

A role in SAP is created by the profile generator (transaction PFCG). Roles provide access to transactions, reports, Web applications, etc. Within each role, you can also view and maintain user assignments. The *rule of least privilege* is a fundamental principle in SAP Security. The rule can be summarized by the notion that a user should be given exactly what is needed to perform the job; not much more and not much less.

## 2.1 Role types

There are two types of SAP roles: *single* and *composite*. Furthermore, single roles can be set up as *reference-derived roles* or *enabler roles*. This section provides a brief overview of each type of role and what each type is used for. Chapter 3 shows how to create each role and maintain it using the profile generator transaction (PFCG).

Single roles provide access to actions and permissions that make up a user's job or a subset of job responsibilities. Actions can be thought of as transactions and permissions thought of as authorization objects and associated field values. Single roles are the most common type of SAP role.

## Actions and permissions example

Sales clerk Todd Levine needs to be able to create and maintain sales orders in SAP. This translates to transaction codes VA01 and VA02. However, Todd can only maintain certain sales doc types (he is not allowed to create return orders) and is only authorized to do so using company code 1000. These limitations are controlled by his explicit access to various authorization objects within his user roles.

Referenced-derived roles are roles that inherit the menu structure, authorization objects, and authorization values from an existing role. Derived roles are often called *child roles*, whereas the imparting role may be called the *parent or master role*. A derived role is useful when you want to mirror the exact same functionality as the master role, but want to manipulate the organizational levels. When creating derived roles, organization levels and user assignments are not passed from the parent to the child. In fact, these are the only role attributes that should be maintained directly in the derived role, all other changes should be maintained in the master role and inherited by the children.

## Reference-derived role example

As noted above, Todd Levine is a sales clerk for company XYZ. However, Todd only needs access to maintain and create sales orders for company code 1000. Marla Levine, however, needs access to maintain and create sales orders for company code 2000. Otherwise, their access should be identical. In this case, a master role, Z_MAINT_SALES_ORDERS_ALL would be created as the parent or imparting role. Two derived roles, Z_MAINT_SALES_ORDERS_1000 and Z_MAINT_SALES_ORDERS_2000 would be maintained as referenced-derived roles.

Many companies use a reference-derived role as a tactical tool to reduce the time and resources necessary for ongoing role maintenance. Reference-derived roles are also used as a case for scalability because they can easily be mixed and matched to fit a business user's job responsibilities and organizational assignments.

An enabler role can be thought of as a bolt-on role. Unlike derived roles, enabler roles are created without any link to an already existing role. Enabler roles have manually added authorization objects added to them with only desired field values maintained.

### Enabler role example

Release strategies are a common example of when enabler roles are useful. An example is when a company wants all purchasing administrators to have access to all purchasing-related activities, but wants to limit the team's access to specific release strategies based on levels. Release strategy authorization is controlled by a single SAP authorization object: M_EINK_FRG which has two fields, Release Code and Release Group. This authorization object can be inactivated within the purchasing admin role and bolt-on enabler roles can be created, one for each Release Code and Release Group combination and assigned ad hoc to each purchasing admin.

A *composite role*, also known as a collective role, is a grouping of two or more single roles. Composite roles are used for the purpose of simplifying the assignment of roles to users. Composite roles do not contain any authorization data, only other roles. Furthermore, composite roles can only be groupings of single roles, not other collective roles.

# 3 Profile generator and role maintenance overview

**This chapter introduces the profile generator transaction, PFCG. The profile generator tool is responsible for enabling the SAP Security administrator to create specific user roles, which contain authorizations to various system functions. Chapter 4 identifies the relationship between profiles, roles, and authorizations and the basic maintenance features within the transaction.**

## 3.1 What is a profile?

The *profile generator* is a tool that creates SAP user roles, which correspond to profiles. Access to the profile generator is via transaction code PFCG. A *profile* is a collection or grouping of SAP authorizations.

**Role definitions**

Best-in-class SAP Security role designs take into account some critical success factors, considering sustainability and scalability are absolutely essential when designing SAP Security roles. Furthermore, involving the business in role content and governance is imperative.

## 3.2 What is an authorization?

The following information is stored in a profile:

### Authorization object classes

- Logical grouping of authorization objects
- Contain one or more authorization objects

# B Index

A

Access Creep 10
Authorization 40
  Authorization Object 40
  Authorization Object Class 39
Authorization Object Security 55
Authorization Trouble-Shooting 73
  ST01,System Trace 76
  SU24, Maintain Check Indicators 84
  SU53, Evaluate Authorization Check 73

C

Central User Administration 34
Composite Role 37, 61
  Creating a Composite Role 61

E

Enabler Role 37

G

Governance Risk and Compliance 91
GRC Access Control 92
  Access Request Management 93
  Access Risk Analysis 92
  Business Role Management 93
  Emergency Access Management 93

P

Passwords 33
  Security Policies 34
Profile 39
Profile Generator 39
  Authorization Tab 47
  Description Tab 46
  Menu Tab 46
  Organizational Levels Window 48
  Role Creation and Profile Generation 45
  User Tab 53

R

Reference-Derived Role 63
  Creating a Derived Role 64
  Transaction Inheritance 46
Roles 35
  Role Types 35
Rule of Least Privilege 10

S

SAP Security Tables 78
  User Information System 87
Security and Authorizations 9
  Basic Architecture 9
  SAP Authorization Concept 10
Security Upgrade 89
Segregation of Duties 68
Sensitive Security Authorizations 80
Single Role 61

**T**

Transporting Roles 68
- Release Transport Request 70

**U**

User Buffer 94

User Groups 16
- User Group Maintenance 26

User Master Record 13
- Address Tab 15
- Defaults Tab 18
- Groups Tab 22
- License Data Tab 22
- Logon Data Tab 15
- Mass Maintenance 27
- Parameters Tab 19
- Personalization Tab 22
- Profiles Tab 21
- Roles Tab 20
- SNC Tab 17
- User ID 13

User Types 24