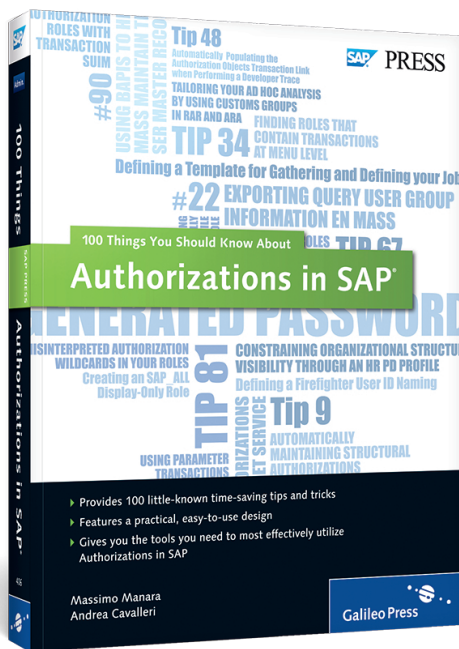


Andrea Cavalleri and Massimo Manara

100 Things You Should Know About Authorizations in SAP®



 Galileo Press®

Bonn • Boston

Contents at a Glance

1	User Master Records	13
2	Development Security	61
3	Profile Generator	103
4	Segregation of Duties	195
5	Upgrades	229
6	Auditing	255
7	Security Templates	287
8	Continuous Compliance and Governance	303

Contents

Acknowledgments	11
PART 1 User Master Records	13
1 Displaying the Technical Names of Transactions in the SAP Easy Access Menu en Masse	15
2 Improving Your User Master Record Accuracy with Hidden Fields	18
3 Defining an SAP User ID Naming Convention to Manage User Master Records	21
4 Using BAPIs to Help Mass-Maintain the User Master Record	23
5 Customizing the Rules for Automatically Generated Passwords During User Creation	27
6 Finding and Using User Parameters to Prepopulate Transactional Fields	30
7 Improving Your Business Reporting through User Groups	33
8 Working with Inactive Users	36
9 Customizing SAP and User Menus through the Session Manager	38
10 Assigning Roles through an Organization Structure without SAP HCM Deployed	40
11 Constraining Organization Structure Visibility through an HR Personnel Development Profile	42
12 Automatically Maintaining Structural Authorizations	45
13 Linking User Master Records to HR Data	48
14 Performing Mass Changes for Users and Roles in Java	51
15 Displaying Authorization Errors in Transaction Log SU53 for Different Users	54
16 Customizing Users' Selection en Masse	56
17 Mass-Changing Secure Network Communications Data for SSO User Mapping	58
PART 2 Development Security	61
18 Validating Your ABAP Code before Moving into the Production System	63
19 Archiving and Restoring a User's Favorites	65
20 Displaying the Security Data Dictionary Definition with the Object Navigator	68
21 Finding Vulnerability Strings in Your ABAP Code	71
22 Creating a Transaction Variant to Restrict User Activities	75

23	Finding Authorization Object Documentation	78
24	Searching for Values and Definitions in ABAP Data Dictionary Tables ...	81
25	Mass-Exporting Query User Group Information	83
26	Managing an Authorization Check in the Transaction Header	86
27	Restricting a User's Access to Called Transactions	88
28	Managing Customizing Tables in a Production System	92
29	Analyzing Your Security System to Keep it Updated	95
30	Using Parameter Transactions to Avoid Giving Direct Tables/Programs Access to End Users	97
31	Discovering Maintenance Customizing Transactions with a Table Name	100
PART 3 Profile Generator		103
32	Finding Roles That Contain Transactions at the Menu Level	105
33	Permanently Enable the Technical Name View in Transaction PFCG's Authorization Tree	107
34	Creating a Sustainable Authorization Roles Naming Convention	110
35	Evaluating the Manual or Modified Authorization Status during Profile Generator Maintenance	116
36	Creating an SAP_ALL Display-Only Role	119
37	Maintaining an Aligned Set of Job Roles with a Naming Convention	123
38	Designing and Assigning a Basic Role to All Users	126
39	Maintaining Derived Roles to Improve Authorization Maintenance	128
40	Discovering Misalignment between Transactions by Downloading Data to Spreadsheets	131
41	Finding Misinterpreted Authorization Wildcards in Your Roles	134
42	Performing Mass Downloads and Uploads of Standard Authorization Values	137
43	Setting Up Mass Adjustments for Derived Roles	139
44	Troubleshooting Authorization Problems for Users	141
45	Customizing Your Tree Menu Settings to Avoid Duplicate Structures ...	145
46	Automatically Populating the Authorization Objects Transaction Link When Performing a Developer Trace	149
47	Adjusting Query Maintenance to Avoid Security Problems	154
48	Cleaning Up Unused Batch Jobs	156
49	Setting Up Authorizations to Allow Internet Service	159
50	Avoiding Security Holes during SAP Menu Role Maintenance	162
51	Changing the Rules to Generate Profile Names	166
52	Comparing Authorization Roles to Check for Alignment Between Systems	168
53	Replacing the Parent Role of a Derived Role en Masse	170
54	Generating Large Quantities of Profiles for Roles in a Single Transaction	173

55	Using SAP BAPIs to Manage Roles with an External Program	176
56	Using Manual Composite Profiles to Bypass the Profile Technical Limit of 312	180
57	Using Parameter IDs and Customizing Transactions to Manage Authorizations	185
58	Removing Expired User-Role Links	189
59	Filtering Roles by Their Status	191
PART 4 Segregation of Duties		195
60	Tailoring Your Ad-Hoc Analysis by Using Custom Groups in RAR and ARA	197
61	Modifying Your Selection Criteria for User/Roles Analysis in SAP GRC 10.0	201
62	Clustering Data to Enhance Your RAR Reporting for Easier Consumption	204
63	Performing a User Impact Risk Analysis	207
64	Setting Selection Criteria for the Web Interface as a Default Value	210
65	Defining a Firefighter User ID Naming Method	212
66	Using Organizational-Level Mapping in Business Role Management to Improve Role Derivation	215
67	Using Business Role Management to Define Business Roles in Place of Composite Roles	219
68	Setting Up Data Segregation in SAP GRC ARA	222
69	Keeping Your Mitigation Tables Clean and Accurate with the Invalid Mitigation Report	226
PART 5 Upgrades		229
70	Making Your Roles Compliant with Transaction SU25	231
71	Deciding How to Set Up Your Authorization Upgrade	237
72	Managing Derived Roles during an Upgrade	241
73	Converting a Manually Created Profile into a Role	244
74	Avoid Maintaining a Role's Authorization Tree Twice When New Transaction Codes Are Added	247
75	Identifying New Transactions in a Role's Menu	249
76	Communicating Password Requirement Changes During SAP Upgrades	251
PART 6 Auditing		255
77	Searching for Roles or Users Using Transaction SUIM with Asterisk Searching	257
78	Using the Security Audit Log to Manage Your Super Users' Access	259

79	Changing the Classification of an Audit Log Message	263
80	Configuring the SAP System to Log Activity in the Security Structure ...	266
81	Activating Table Tracing to Log the Details of Changes Made	269
82	Viewing All Instances of Profile Parameters	272
83	Identifying Alias Transactions to Eliminate Unauthorized System Access	275
84	Finding a Specific User Who Has Made Changes to Values	279
85	Identifying Query Changes	282
86	Protecting and Auditing Your Remote Function Call	284
PART 7 Security Templates		287
87	Using a Spreadsheet to Collect Authorization Data	288
88	Defining a Template for Gathering and Defining Your Job Role Data	291
89	Defining a Template for Gathering the Organizational Constraints of Job Role Data	294
90	Defining a Template for Gathering the Nonorganizational Constraints of Job Role Data	297
91	Using Pivot Tables and Authorization Reports to Customize Data for the Reader	300
PART 8 Continuous Compliance and Governance		303
92	Defining Data for User Revalidation	305
93	Revalidating Roles and Providing Documentation for Analysis	309
94	Making Sure Users Are Assigned Only to the Roles and Transactions They Use	312
95	Using Indirect Role Assignment to Simplify User Maintenance and Reporting	315
96	Defining Business Owners	319
97	Finding Misalignments between Organizational-Level Pop-Ups and Authorization Data in Derived Roles	321
98	Finding Manually Created Authorizations in a Role's Authorization Tree	325
99	Substituting SAP Queries with Specific Transaction Codes	328
100	Using a Query to Find Manually Created Authorizations and Convert them to Roles	330
Additional Resources		333
Index		339

Creating an SAP_ALL Display-Only Role

Using Transaction PFCG, you can create a role that provides display-only user access starting with an existing profile.

You should have a wide range of authorization roles to display the system and configuration data in various situations; for example, to assign roles to consultants for a startup and analysis project in development and quality/training systems. You can use Transaction PFCG to create these kinds of roles and ensure display-only access.

And Here's How ...

To create an empty role, access Transaction PFCG (Change Roles), and go to the AUTHORIZATIONS tab (see Figure 1).

The system will ask if you want to use a predefined authorization model. If you want to select a template to fill the AUTHORIZATION tab, choose the SAP_ALL template profile, and then click on ADOPT REFERENCE (Figure 2). In this way, all authorizations entered in the SAP_ALL profile are used to fill up the role.

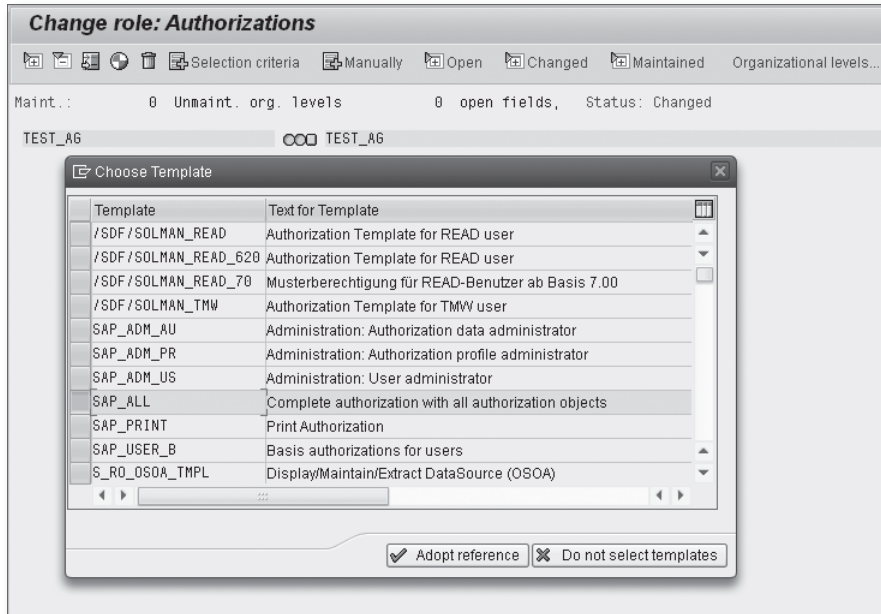


Figure 1 Choose Template Pop-Up Screen

Alternatively, when you are in the authorization tree, you can use the following menu path to enter all authorizations:

EDIT • INSERT AUTHORIZATION(S) • FULL AUTHORIZATION

By doing this, you can ensure that all authorization objects that are entered in the SAP_ALL profile are covered by the role that you are creating.

Next, ensure that this role lets the user access the system in display mode only. Use Table TACT to discover all possible activity entries for the ACTVT field. Common display activity codes are 03 (display), 04 (print), 08 (display changes documents), and 09 (display prices). Activity codes 27, 28, 29, 53, and 54 display activities mainly used in the Controlling (CO) module; 33 reads on the file system directory. Be sure that in all authorization objects with the ACTVT field, the values chosen are in display.

Look for all authorization object fields with the ACTVT field, and set them in display mode by entering the previously listed values (see Figure 2). To do this, click on the binoculars icon, and then find all authorization objects with the ACTVT field.

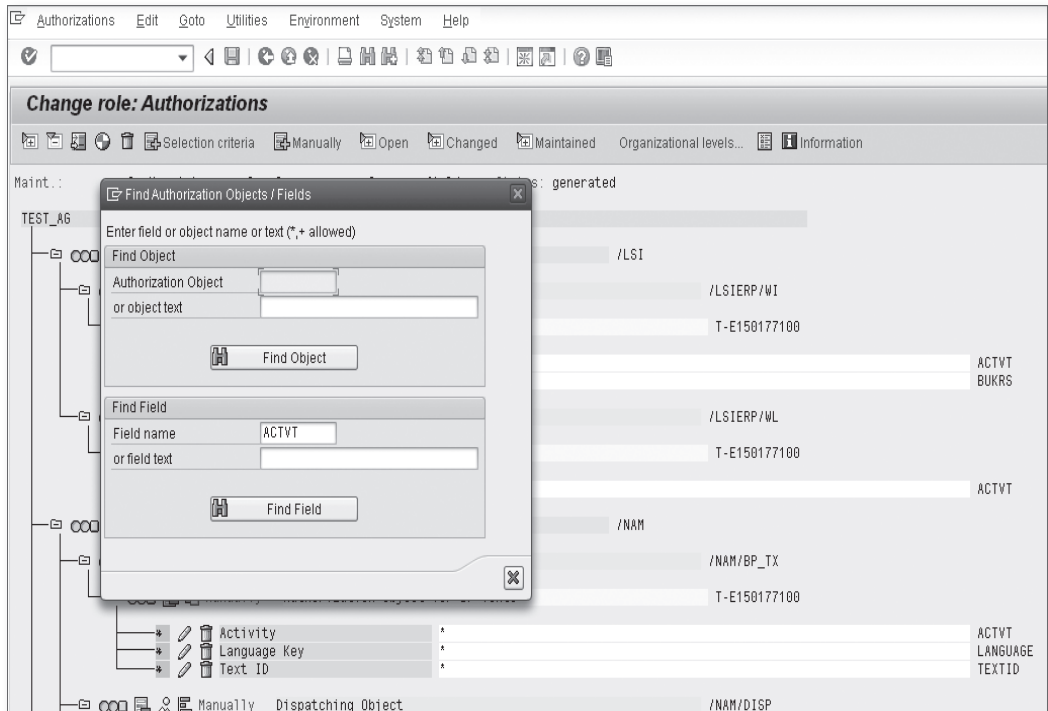


Figure 2 Display Authorizations with the ACTVT Field

If the ACTVT values entered are only in write mode for a certain authorization object, you have to deactivate the object. This is time consuming but is a one-time process. At the end of this setup activity, check whether all values are properly deactivated by accessing Transaction SE16 and browsing Table AGR_1251. Enter your role name in the AGR_NAME field, enter the value "ACTVT" in the FIELD field, and exclude all display values previously listed (03, 04, 08, etc.) in the LOW field. The query in Figure 3 shows you all of the authorization objects where ACTVT is not in the display mode values.

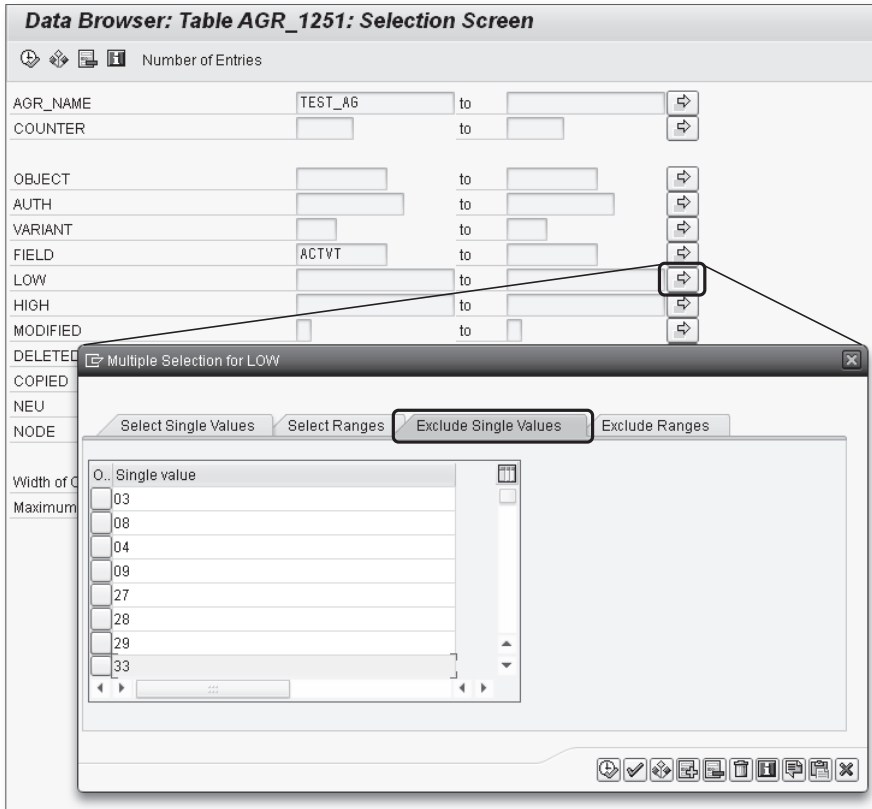


Figure 3 Browsing Table AGR_1251 with Transaction SE16

Note that not all authorization objects have an ACTVT field for managing the activity; in the HR component, the ACTVT field is AUTHC, where the value “R” means read mode. It’s also a good approach to disable all authorization objects that are critical, based on your internal policy for your company. You can also limit transaction execution by entering a range in S_TCODE authorization objects (e.g., if this role should be allowed to run all transaction except Transaction PFCG). Keep in mind that a range approach can decrease governance because it’s more difficult to document the roles and be aware of what the roles allow.

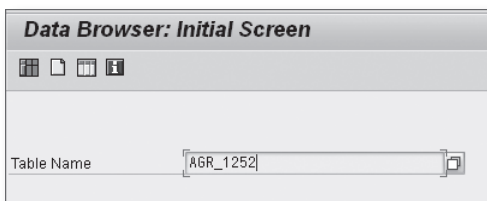
Finding Misinterpreted Authorization Wildcards in Your Roles

You can find wildcard values in your roles by browsing SAP tables and using Microsoft Excel or Access to export your results.

You can use wildcard characters in authorization values. However, if an authorization value contains other characters after an asterisk, the SAP kernel ignores these characters during the authorization check. For example, the value A*B* is actually interpreted as A*. You can find these cases quickly by browsing SAP tables and exporting your findings for analysis through Microsoft Excel or Access.

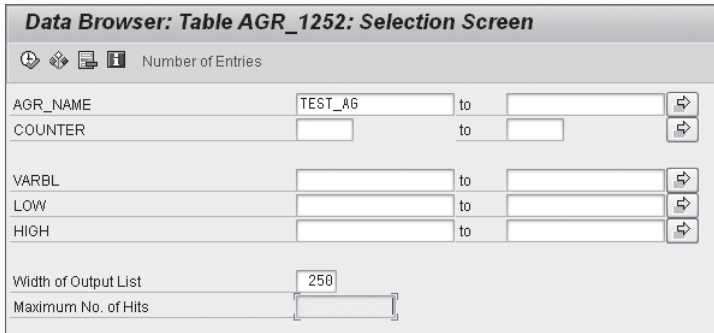
✓ And Here's How ...

Through Transaction SE16, you can directly browse SAP tables that contain the authorization objects and values of a role (shown in Figure 1). You can also browse Tables AGR_1251 or AGR_1252. This example shows you how to find which authorization values in your system contain wildcards that have not properly been set up via Table AGR_1252, which contains the organizational authorization level values for a role. Fill in the TABLE NAME field and press .



« Figure 1 Execute Transaction SE16 on Table AGR_1252

In the selection screen interface (see Figure 2), enter your role name in the AGR_NAME field and press **F8**.



« **Figure 2**
Transaction SE16
Selection Screen

As a result, you can see all authorization organization values in this role (see Figure 3).

MAN...	AGR_NAME	COUNT...	VARBL	LOW	HIGH
001	TEST_AG	1	\$BEGRP	*	
001	TEST_AG	2	\$BUKRS	AA*B	
001	TEST_AG	3	\$BWKEY	*	
001	TEST_AG	4	\$EKGRP	*GB	
001	TEST_AG	5	\$EKORG	F*F	
001	TEST_AG	6	\$IWERK	*	
001	TEST_AG	7	\$KKBER	*	
001	TEST_AG	8	\$KOART	*	
001	TEST_AG	9	\$KOKRS	A01*	
001	TEST_AG	10	\$KOSTL	*	
001	TEST_AG	11	\$LGNUM	*	
001	TEST_AG	12	\$LGTYP	*	
001	TEST_AG	13	\$PLVAR	*	
001	TEST_AG	14	\$SPART	*	
001	TEST_AG	15	\$SWERK	*	
001	TEST_AG	16	\$VKBUR	*	
001	TEST_AG	17	\$VKGRP	*	
001	TEST_AG	18	\$VKORG	*P01	
001	TEST_AG	19	\$VSTEL	*	
001	TEST_AG	20	\$VTWEG	A0	
001	TEST_AG	21	\$WERKS	*	

« **Figure 3**
Organization
Authorization Values in
Role TEST_AG and the
Local File

Export this table into an Excel spreadsheet by clicking on the LOCAL FILE icon circled in Figure 3, and then choosing the SPREADSHEET checkbox. Use a formula (such as “=IF(ISERROR(IF(FIND(“*”;D2)<>LEN(D2);”ERROR”;””));””);IF(FIND(“*“

Troubleshooting Authorization Problems for Users

As an administrator, you can monitor and analyze an authorization problem during a user session with Transaction ST01.

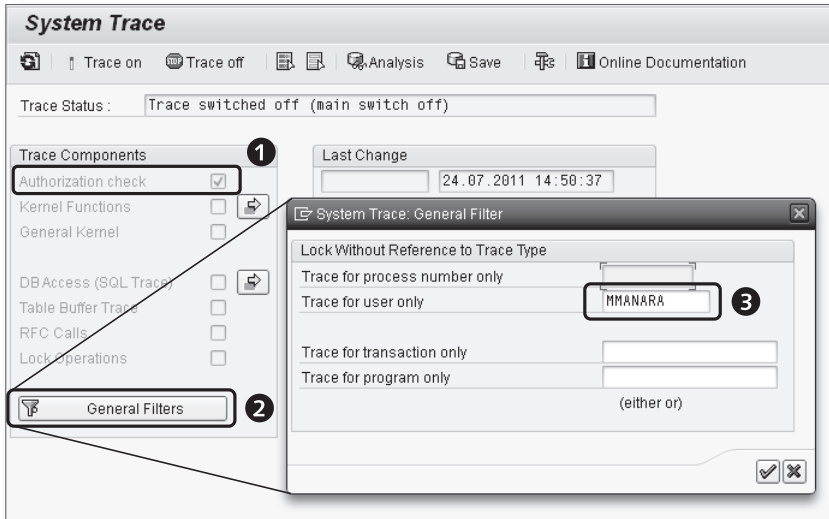
In normal cases, when a user receives an authorization error, the end user or administrator will execute Transaction SU53; this transaction shows that the last authorization check failed. However, you'll find that this error log isn't sufficient to resolve the problem when working with custom or standard transactions. In these cases, you'll find it necessary to perform an authorization trace during a user session with Transaction ST01.

And Here's How ...

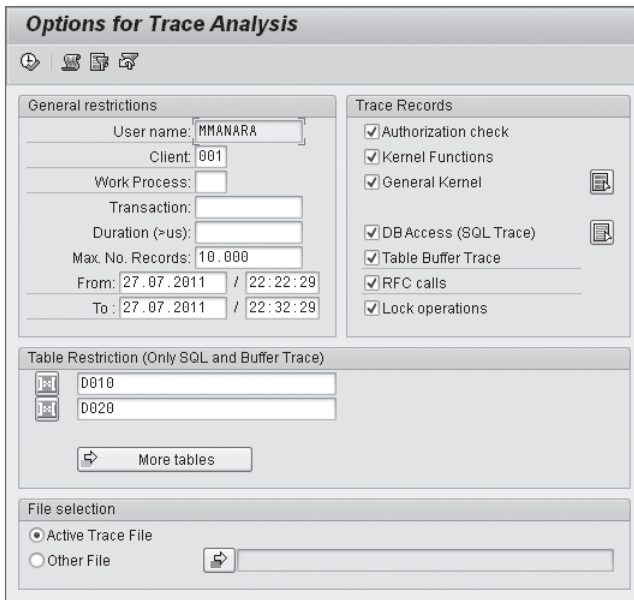
To place a trace on a user, execute Transaction ST01 and flag the AUTHORIZATION CHECK indicator under the TRACE COMPONENTS box (❶). Click on the GENERAL FILTERS button (❷), and enter the user ID in the TRACE FOR USER ONLY field (❸, see Figure 1).

After setting Transaction ST01 filters, click on the TRACE ON button. From this moment until you click on TRACE OFF, all activities performed by the user MMANARA are logged depending on your earlier settings (in this case, only whether the authorization check passed and failed).

After the user completes the test session and after you terminate the trace, you can analyze the activities performed by the trace by clicking on the ANALYSIS button. The system shows you the analysis filter selections (see Figure 2) where you have to enter the test user ID and type .



⤴ Figure 1 Setting Up Transaction ST01 Filters



⤵ Figure 2 Selection Criteria in Trace Analysis

You'll now see the log that shows all authorization checks that have been performed in Figure 3. If the return code equals zero, the authorization check has passed. If the value is different from zero, the authorization check failed.

Trace Display				
hh:mm:ss.ms	Type	Lasts(us)	Object	Text
Client: 001 User: MMANARA Transaction 77A7CB7055D94E97941BCE3907FD11EF				
Work Process 1 PID Date: 27.07.2011 Start: 22:25:49:410.659Finish: 22:25:49:337.877				
First Block of Dialog Step Last Block in Dialog Step				
Block Version: 4234 No. of Records: 17 File Version: 1				
hh:mm:ss.ms	Type	Lasts(us)	Object	Text
22:25:49:411	AUTH	- - -	S_TCODE RC=0	TCD=MM03;
22:25:49:636	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM= ;
22:25:52:451	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=K;
22:25:52:476	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=D;
22:25:52:481	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=E;
22:25:52:484	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=A;
22:25:52:489	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=L;
22:25:52:491	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=B;
22:25:52:494	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=S;
22:25:52:497	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=Z;
22:25:52:499	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=X;
22:25:52:501	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=V;
22:25:52:504	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=P;
22:25:52:506	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=C;
22:25:52:518	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=F;
22:25:52:522	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=Q;
22:25:52:525	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=G;
Client: 001 User: MMANARA Transaction MM03 C829093DF81F4257BDE4EC7ACAA26CFD				
Work Process 1 PID Date: 27.07.2011 Start: 22:25:59:95.868Finish: 22:25:59:569.749				
First Block of Dialog Step Last Block in Dialog Step				
Block Version: 612 No. of Records: 1 File Version: 1				
hh:mm:ss.ms	Type	Lasts(us)	Object	Text
22:25:59:96	AUTH	- - -	S_PROJECT RC=0	PROJECT_ID= ;APPL_COMP= ;PROJ_CONF= ;ACTVT= ;
Client: 001 User: MMANARA Transaction 77A7CB7055D94E97941BCE3907FD11EF				
Work Process 1 PID Date: 27.07.2011 Start: 22:26:15:62.898Finish: 22:26:15:389.938				
First Block of Dialog Step Last Block in Dialog Step				
Block Version: 724 No. of Records: 2 File Version: 1				
hh:mm:ss.ms	Type	Lasts(us)	Object	Text

⌘ **Figure 3** Authorization Trace Log

Let's quickly review a few important things to keep in mind when using Transaction ST01:

- ▶ Transaction ST01 is application server dependent. In other words, if your system has more than one application server (you can determine this by using Transaction SM51), you have to be sure that the Transaction ST01 trace is performed in the same application server the user is logged into. To do that, in Transaction SM51, you can perform a remote logon to another application server by typing **[Ctrl]+[Shift]+[F8]** (see Figure 4).
- ▶ Take a look at your time zone and clock. If the application server has a time that is different from your PC, then during your analysis, after performing the trace, you might select a trace log outside the time recorded.

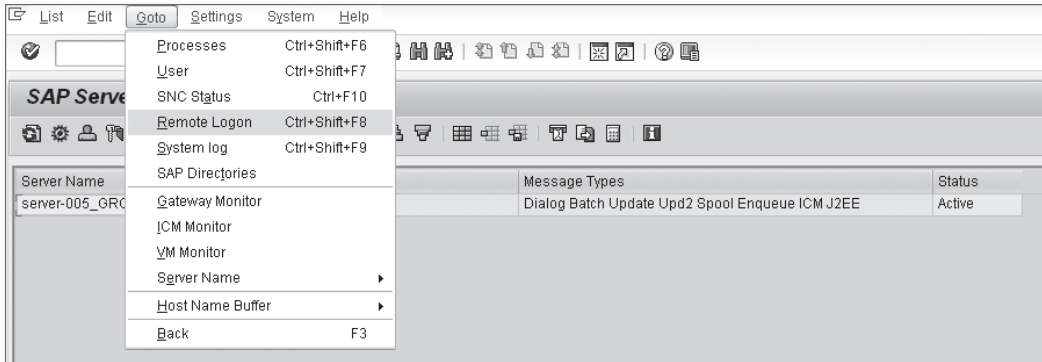


Figure 4 Perform a Remote Logon in Transaction SM51

- ▶ You can view in what application server a user is currently logged in to by using Transaction AL08 or by asking the user directly—he can see the application server name in the bottom-right area of your SAP GUI (Figure 5).

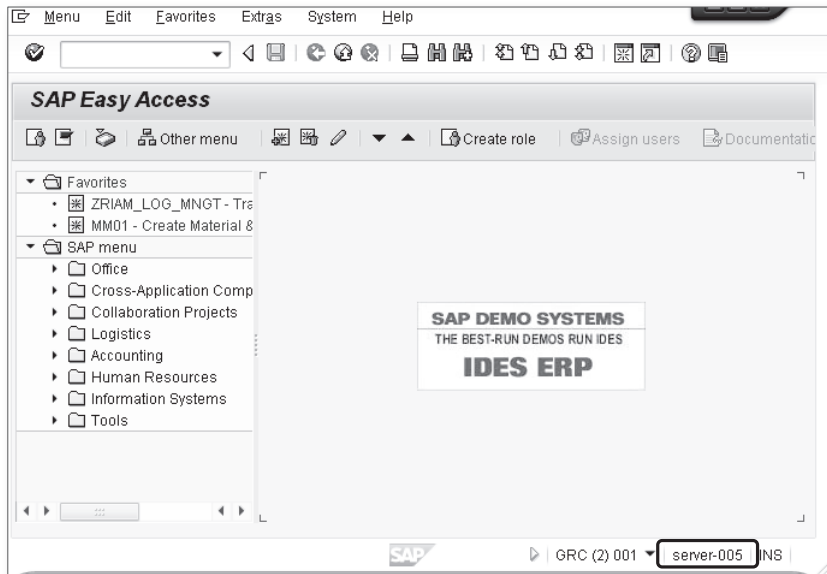


Figure 5 Discover the Application Server a User Is Logged In To

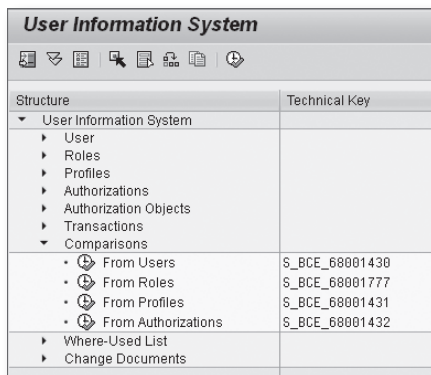
Comparing Authorization Roles to Check for Alignment Between Systems

You can easily compare two roles in different systems and check for alignment by using Transaction SUIM.

Comparing authorization roles is not a simple task if these roles contain several authorizations. Sometimes you may need to compare the same role if they have different values in the development system and quality system. This misalignment by the system is not in compliance using the transport management system. Through Transaction SUIM, you can easily compare two roles in a system or cross system.

✓ And Here's How ...

Access Transaction SUIM to display the COMPARISONS tree shown in Figure 1.



Structure	Technical Key
<ul style="list-style-type: none"> ▼ User Information System <ul style="list-style-type: none"> ▶ User ▶ Roles ▶ Profiles ▶ Authorizations ▶ Authorization Objects ▶ Transactions ▼ Comparisons <ul style="list-style-type: none"> • From Users • From Roles • From Profiles • From Authorizations ▶ Where-Used List ▶ Change Documents 	<ul style="list-style-type: none"> S_BCE_68001430 S_BCE_68001777 S_BCE_68001431 S_BCE_68001432

« Figure 1 Transaction SUIM Comparisons Tree

Click on FROM ROLES S_BCE_68001777. The screen shown in Figure 2 appears. Enter the role names you want to compare in the ROLE A and ROLE B fields.

Figure 2 Role Comparison

Specify the system where you want the comparison performed by clicking on the ACROSS SYSTEMS button and then choosing the system ID name from the system list. For example, you can compare a role in the development system and a role in the production system. Note that to perform this functionality correctly, it's essential that the system's remote function call (RFC) destinations are defined.

The result of the comparison is shown in Figure 3. The COMPARISON column can display three different colors: Red means that different authorization objects exist between the roles, yellow indicates that the different roles have the same authorization objects but different values, and green indicates that the roles have the same authorization objects and same values. If the comparison is all green, that means the roles are equal. If you're seeing red or yellow, you can use Transaction PFCG to correct it.

Comparison	Object	Operand 1	Operand 2	Authorization Object Name
Red	C_CLAS_NRM	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Load Standards Data
Red	C_CLAS_UMS	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Class Split/Merge
Red	C_CLAS_UTI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization for Class Utilities
Green	C_DRAD_OBJ	<input type="checkbox"/>	<input type="checkbox"/>	Create/Change/Display/Delete Object Link
Red	C_DRAW_BGR	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization for authorization groups
Red	C_DRAW_DOK	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization for document access
Red	C_DRAW_MUP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization for Markups
Red	C_DRAW_STA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization for document status

Figure 3 Comparison Result Example

Unfortunately, this transaction doesn't support a mass comparison between several roles at one time. However, you can go to www.sdn.sap.com, where you can find information on an enhancement that works around this limitation.

Index

A

- ABAP code, 17
- ABAP Data Dictionary, 68
 - tables*, 81
- ABAP program, 71, 151, 250
- ABAP programming language, 63
- ABAP scan, 63
- ABAP source code, 282
- ABAP statement, 89
- ACTVT values, 121
- Ad-hoc risk analysis, 197
- Administrative function, 127
- Algorithm
 - MD5*, 251
 - SHA1*, 251
- Alias transactions, 275
- Analysis, 176
 - phase*, 176
- Application server, 144
 - dependent*, 143
- Approval step, 269
- ARIS, 291
- Assign roles, 45
- Asterisk, 134, 162, 257, 296
- Audit, 275
 - class*, 263
- Audit Information System (AIS), 281
- Authority check, 238
- Authorization
 - check flow*, 86
 - data*, 288
 - element*, 107, 108
 - error check*, 54
 - error message*, 224
 - group*, 329
 - manage*, 185
 - management*, 277
 - model*, 119
 - modify*, 231
- Authorization (Cont.)
 - profiles*, 181
 - template*, 287
 - tree*, 247, 325
 - troubleshooting*, 54
 - upgrade*, 229
 - value*, 134, 137
- Authorization object, 149, 298
 - constraints*, 100
 - documentation*, 78
 - field*, 299
 - GRAC_FUNC*, 222
 - GRAC_RISK*, 222
 - S_DEVELOP*, 127
 - S_GUI*, 127
 - S_TABU_DIS*, 257
 - S_TABU_NAM*, 154
 - S_TCODE*, 106, 122, 131, 164, 310
 - values*, 126
- Authorization role, 112
 - compare*, 168
- Authorization status, 116
 - best practice*, 235
 - maintained*, 116
 - manual*, 116
 - modified*, 116
 - standard*, 116
- Authorization trace, 141
 - auth/authorization_trace*, 149

B

- Backdoor, 63
- Background job, 140
- Backup, 137
- BAPI, 23, 176, 177
 - import parameters*, 25
- Basic activity, 126
- Basis role, 284

Boolean field, 111
BRM mapping, 216
Business area owner, 320
Business contact, 315
Business department, 40
Business description, 291
Business intelligence, 155
Business process owner, 204, 300, 320
Business revalidation, 310
Business role, 219
 definition, 221
Business transaction, 127
Buyer, 182

C

Called transaction, 71, 88
Case-sensitivity, 251
Change document, 267, 279
Change request, 173
Child value, 216
Classify output results, 205
Client-dependent key, 167
Client role, 92
Client-specific, 84
Cluster data, 204
Code Inspector, 63
Color, 290
Company code, 31
Comparison, 169
Composite roles, 114, 182, 219, 308
Computer Aided Test Tool (CATT), 172
Concatenate, 132
Convert profile, 244
Copy SAP data, 153
Cost center, 306
Counter, 112
Country code, 114
C program, 64
Cross-client, 84
Custom development, 70
Customer tables switch, 238
Customize tables, 92
Customizing objects changes, 269
Customizing projects, 101

Customizing switch, 16, 28, 42, 100
Customizing transaction, 276
Customizing tree, 101
Custom table, 269
Custom transaction, 77, 137, 149
Custom user group, 198

D

Data collecting, 291
Data domain, 128, 321
Data mart, 205
Data owner, 320
Data segregation, 222
Default value, 210
Delete user, 66
Department, 306
Derive composite role, 124
Derived role, 170, 217, 241, 310, 321
 grouping, 182
 upgrade, 241
Determine errors, 115
Developer trace, 153
Development system, 167
Dialog users, 284
Different periods, 189
Display-only user access, 119
Documenting authorization, 300
Document type, 297
Download functionality, 138
Dummy entries, 163, 226
Duplicated record menu, 147
Dynamic configuration, 260

E

Edit, 113
Emergency user, 212, 259
Employee departure, 36
Enterprise Role Management (ERM), 215
Evaluation path, 317
Exceptions, 39
Exchange rates maintenance, 92
Exclude objects, 204

Execute program, 97
 Expiration date, 37
 Expired, 37
 role, 190
 External software programs, 159

F

Father role, 170, 171
 Field
 ACTVT, 120
 Filters, 273
 Financial period-end closing, 92
 Firefighter naming convention, 212
 Firefighter user ID (FF ID), 212
 Formula, 133
 Function group, 285
 Function maintenance, 222
 Function module, 16, 66, 83
 RSAQ_IMPORT_USERGROUP_CATALOG,
 84
 PRGN_SET_BROWSER_OPTIONS_USER,
 16

G

Generate button, 175
 Generated profile, 175
 Generated query, 332
 program, 329
 Global setting, 147
 Go-live, 176

H

Help desk, 251
 History table, 37
 HR component, 122
 HR data, 18, 48
 HR department, 292
 HR-OM, 306, 315
 HR repository, 18

HR system, 306
 HTTP, 159
 Human Resources, 306

I

Identical to profile
 method, 246
 option, 245
 Identity management, 307
 Implementation, 176
 Import a role, 191
 Indirect assignment, 40
 Infotype, 266
 0105, 306
 Infotype 0105, 48
 Inheritance relationship, 171
 Instance parameter, 149, 272
 Internet Communication Framework (ICF),
 159
 Invalid Mitigating Controls, 226

J

Java, 51
 role, 52
 Java Database Connectivity (JDBC), 205
 Job, 306
 authorization, 156
 scheduled, 37
 Job role, 123, 295
 architecture, 124
 master list, 292
 Join query, 308

L

Level of abstraction, 221
 Lightweight Directory Access Protocol
 (LDAP), 205
 Link transaction code to the query, 329
 Localized job role, 125
 Locked, 37

- Lock users, 36
- Log, 263
- Log Data Changes, 270
- Logging, 266
 - event*, 263
- Logon language, 311
- Lookup formula, 132

M

- Maintain table, 97
- Management, 112
- Manual authorization, 118, 327
- Manual composite profile, 183, 184
- Manually created authorizations, 330
- Manually created profile, 244
- Manually create roles, 215
- Manual profile, 332
- Mass download, 138
- Mass output, 173
- Master language, 301
- Material master data view, 297
- Maximum number of profiles, 180
- Menu level, 105
- Menu policy, 38
- Menu tree, 165
- Merge & Center functionality, 290
- Microsoft Access, 295
- Microsoft Excel, 134, 193
 - spreadsheet*, 135
- Microsoft Excel macro, 299
- Microsoft Office, 288
- Misalignment, 133
 - role menu and S_TCODE*, 133
- Mitigation table, 226
- Modified authorization, 117
- Monitor users, 284
- Multiple spreadsheets, 290

N

- Naming convention, 110, 111, 123
- National or international laws, 22
- New authorization values, 248

- New role, 177
- New transaction codes, 247, 249
- Nondialog user, 284
- Nonorganizational constraints, 297
- Non organization fields, 130
- Number ranges, 167

O

- Object
 - S_QUERY*, 155
 - S_TABU_NAM*, 328
 - S_USER_GRP*, 34, 55
- Object Navigator, 68
- Obsolete roles, 190
- Office software tool, 288
- Open Office, 288
- Optimized option, 245
- Organizational constraint, 297
- Organizational field, 295
- Organizational level, 129, 311
 - constraint*, 294
 - field*, 322
 - mapping*, 216
 - pop-up*, 321, 322
- Organizational panel, 324
- Organizational structure, 40, 266, 318
- Originals only, 138

P

- Parameter settings, 188
- Parameter transaction, 97
- Parent role, 111, 128, 129, 242
- Password, 251, 284
 - minimum length*, 252
 - requirement changes*, 251
- Pattern language, 113
- Performance, 63
- Periodic job, 156
- Periodic revalidation, 319
- Permission, 51
- Personnel development (PD) profile, 42, 45
- Personnel master record, 48

Pivot table, 315
tool, 300
 Position level, 40
 Prepopulate fields, 30
 PRGN, 176
 Primary organizational level, 216
 Principle of least privilege, 312
 Privacy law, 262
 Production landscape, 63
 Production system, 92, 166
 Professional layout, 302
 Profile, 166, 244, 332
 naming, 166
 naming rule, 166
 status, 192
 Program
 PRGN_COMPRESS_TIMES, 189
 SUPRN_REGENERATE_DEPENDENT, 140
 Purchase order, 187

Q

Query, 282
 area, 83
 authorization group, 83
 maintenance, 154
 strategy, 155
 technical name, 282
 user group, 84, 155
 Quick Viewer, 332

R

Random password, 27
 Reboot system, 150
 Recurrence level, 72
 Relational database management system
 (RDBMS), 288
 Remote function call (RFC), 169, 178, 284
 connection, 212, 285
 destination, 286
 logon, 260
 Report
 RHCDOC_DISPLAY, 267

Report (Cont.)
 RSECNOTE, 95
 RSPARAM, 90, 272
 RSRFCCHK, 286
 Reporting framework, 204
 Repository object, 69
 Retention period, 313
 Return on investment (ROI), 125
 Revalidation, 319
 Risk Analysis interface, 226
 Risk Analysis reporting, 204
 Role, 191, 312
 adjustment, 130
 analysis, 201
 assign, 316
 assigned directly, 111
 authorization tree, 326
 child, 139, 140
 classify, 110
 complexity, 219
 composite, 111, 301
 content, 113
 derived, 111, 128, 139
 duplicated, 189
 empty, 119
 exception, 111
 expired, 189
 level, 207
 maintenance, 162
 mapping feature, 219
 mass-manage, 178
 menu, 106, 131, 145
 owner, 320
 process, 319
 revalidation, 309
 simple, 111, 301
 structure, 221
 template, 139
 upgrade, 231, 240
 Role-based access control (RBAC), 309, 319
 Role menu, 234, 247
 change, 248
 Root name, 40
 Routine, 72
 Rule name, 186

S

SAP_ALL template, 119
 SAP BusinessObjects, 155
 SAP BusinessObjects governance, risk, and compliance (SAP GRC), 195, 259
 SAP documentation, 153
 SAP Easy Access, 15, 38
 SAP ERP HCM, 18, 48
 SAP generated password, 27
 SAP GRC Access Control 5.3 (Superuser Privilege Management), 212
 SAP GRC Access Control Access Risk Analysis, 197
 tables, 206
 SAP GRC Access Control release 10.0 (Emergency Access Management[EAM]), 212
 SAP GRC Access Control Risk Analysis and Remediation, 197
 SAP GRC synchronization, 209
 SAP GUI, 15, 88, 252
 SAP kernel, 134
 SAP menu, 164
 SAP module, 112
 SAP NetWeaver Business Client, 201, 220
 SAP Object Navigator, 68
 SAP Office, 127
 SAP program, 70, 282
 SAP Query, 154, 155, 301, 328
 SAP security concept, 123
 SAP service, 161
 SAP Solution Manager, 291
 SAP standard menu, 39, 145, 162
 SAP updates, 95, 251
 SAP user ID, 21
 SAP User Management Engine (UME), 51
 Screen layout, 75
 Search criteria, 210
 Secondary Organizational Level, 217
 Secure Network Communications (SNC), 58
 Security Audit Log, 259, 263
 Security concept, 110
 Security level, 263
 Security note, 95
 Security template, 288

Segregation of Duties (SoD), 37, 125, 126, 162, 182, 183, 195, 259, 275, 319
 conflict, 182
 mitigation control owner, 320
 risk owner, 320
 rules owner, 320
 Service authorization, 161
 Services tree, 159
 Session manager, 38
 Simple role, 183
 library, 182
 Simulate changes, 207
 Single quotation mark, 258
 Single Sign-On (SSO), 58, 252
 SNC name, 60
 Source code, 178
 Spreadsheet, 131, 288
 Standard authorization role assignment, 45
 Standard report, 302
 Static configuration, 260
 String search, 71
 Structural profile, 45
 System call, 71
 System copy, 167
 System ID, 166
 System parameter, 90

T

Table
 AGR_1251, 116, 131, 134, 286, 311, 324
 AGR_1252, 134, 311, 324
 AGR_AGRS, 125, 301, 311
 AGR_DATEU, 16
 AGR_DEFINE, 301
 AGR_HIER, 164
 AGR_NUM_2, 167
 AGR_TCODES, 131, 301, 311
 AGR_TEXTS, 111, 301, 311
 AGR_USERS, 315
 CDHDR, 279
 CDPOS, 279
 D010SINF, 282

Table (Cont.)

PRGN_CORR2, 249
SSM_CUST, 147
T77CDOC_CUST, 266
T77UA, 44
TBTCP, 157
TBTCS, 157
TCDCOUPLES, 89
TOBJ, 285
TPR_PREF, 109
TSTC, 301
TSTCP, 98
TSTCT, 301
USERTCODE, 314
USOBHASH, 160
USOBT, 138, 239, 240
USOBT_C, 137, 138, 151, 294, 298, 325
USOBX, 138, 240
USOBX_C, 238
USORG_DB, 294
USR04, 181, 183
ZCONVERT_USER, 270

Table log, 269

Table tracing, 269

Technical authorization objects, 107

Technical name, 107, 111

Technical revalidation, 309

Technical transaction name, 15

Template

define, 291

Test, 176

Text file, 51, 67

Trace, 141, 259

Traffic light icon, 191

Transaction

AUTH_DISPLAY_OBJECTS, 78

ME21N, 188

MM01, 321

MM03, 238

OMET, 185

OOSB, 43

PFCG, 78, 104, 215, 232, 248, 277, 298,
325

PFUD, 41

PPOC, 40

Transaction (Cont.)

PPOSW, 316

PPSS, 317

replace, 248

RZ11, 149

SA38, 272

SCC4, 92

SCU3, 271

SE13, 270

SE16, 81, 134, 286

SE37, 176

SE38, 63, 140

SE61, 253

SE80, 23, 68

SE92, 264

SE93, 77, 86, 97

SE97, 88, 89

SHD0, 75

SICF, 159

SM19, 260, 263

SM20N, 261

SM30, 100

SM37, 156

SM51, 143

SNC1, 58

SOBJ, 92

SPRO, 101, 216, 219

*SQ**, 84

SQ00, 85, 155, 282

SQ01, 329

SQ03, 155

SQVI, 308

ST01, 141, 153

ST03N, 312

ST13, 95

SU01, 18, 24, 41, 187, 213, 275, 307

SU02, 277

SU3, 32, 188, 277

SU10, 23, 56, 275

SU22, 152

SU24, 137, 149, 236, 325

SU25, 231, 241, 244

SU50, 32, 188

SU53, 54, 126, 141

SUGR, 33

Transaction (Cont.)
 SUIM, 35, 133, 168, 257
 SUPC, 173
 TABLE_SCANNER, 82
Transaction button, 105
Transaction fields, 32
Transaction header, 86
Transaction SU25
 interface, 237
 step 2, 247
 step 2a, 231
 step 2b, 231
 step 2c, 232
 step 2d, 232, 249
 step 6, 244
Transaction variant, 75
Transport, 166
 all roles, 173
 management system, 168
T-string, 167

U

Unsubstituted value, 273
Upgrade, 75, 231
 phase, 131
 project, 229
Upload functionality, 137
User analysis, 201

User assignments, 189
User attributes, 56
User favorites, 65
User groups, 33
User ID, 181
 assign, 316
 batch, 158
 credential, 286
 delete, 156
User impact analysis, 207
User master record, 14, 190, 305
User menu, 39
User-naming convention, 21
User parameter ID, 30
User process, 319
User revalidation, 305
User session, 141

V

Validity date concept, 189
Visual Basic, 178

W

Wildcard, 134, 189, 191, 259
Workload, 312
Wrap text, 290