This document shows the description of all checks which are executed by the SAP Security Optimization Service for an **ABAP system**.

The check ids are marked in red.

Author: Global Service and Support – Security Services
Contact: securitycheck@sap.com
Date: 10.03.2016
1 SC_INIT - INITIALIZATIONS FOR SECURITY CHECK

1.0.1 Preface .............................................................. 12
1.1 DETECTED ISSUES .................................................... 12

1.2 SPECIAL FOCUS CHECKS ............................................. 13
1.2.1 Compare Clients From Download to Questionnaire Data ......... 13
1.2.2 Client Overview .................................................. 13
1.2.3 Additional Super User Accounts Found (0022) .............. 13
1.2.4 Users - Other Than System Administrators - Are Allowed to Call ST14 (0168) .... 14

2 SC_AUTHENTICATION - SC AUTHENTICATION CHECKS ................. 15

2.1 AUTHENTICATION .................................................... 15
2.1.1 Password Logon Is at Least Partly Allowed (0139) ............ 15
2.1.2 Password Policy .................................................. 15
2.1.2.1 Password Complexity ....................................... 15
2.1.2.1.1 Minimum Password Length (0126) .................... 15
2.1.2.1.2 Character Category Settings (AU093) ................. 15
2.1.2.1.3 Trivial Passwords Are Not Sufficiently Prohibited (0125) 16
2.1.2.2 Initial Passwords .............................................. 16
2.1.2.2.1 Validity of Initial Passwords ....................... 16
2.1.2.2.2 Users with Initial Passwords Who Have Never Logged On (0009) 17
2.1.2.2.3 Users with Reset Password Who Have Not Logged On (0140) 17
2.1.2.3 Interval for Logon with Productive Password Is Too Long (AU081) .... 17
2.1.2.3.1 login/password_max_idleproductive .................. 18
2.1.2.4 Interval for Password Change Is Too Long (0127) ......... 18
2.1.2.5 Too Many Invalid Logon Attempts Allowed Before a Session Is Terminated (0132) .... 19
2.1.2.6 Too Many Incorrect Logon Attempts Allowed Before a User Is Locked (0133) .... 19
2.1.2.7 User Locks due to Failed Logon Attempts Are Automatically Released at Midnight (0134) ......................... 19
2.1.2.8 Security Attack Indicated by Users Locked due to Incorrect Logon Attempts (0141) .... 20
2.1.3 General Authentication ........................................... 20
2.1.3.1 Users Who Have Not Logged On for an Extended Period of Time (0010) .......... 20
2.1.3.2 Security Critical Events for End Users Are Not Logged in the Security Audit Log (0136) .... 20
2.1.3.3 Interval After Which Inactive Users Are Logged Off Is Too Long (0137) .......... 21
2.1.3.4 Multiple Logons Using the Same User ID Is Not Prevented (0138) ............. 21
2.1.3.5 Users - Other Than User Administrators - Are Authorized to Change Passwords (0121) ..... 21
2.1.3.6 Users - Other Than User Administrators - Are Authorized to Lock/Unlock Users (0135) ..... 22
2.1.4 Password Based Authentication Admits Password Attacks (0591) ........... 22
2.1.5 SAP GUI Single Sign-On (SSO) .................................. 23
2.1.5.1 Password Logon Is Allowed to SNC Enabled Servers (0592) .......... 23
2.1.5.2 SNC Users Do Not Have to Change Their Initial Password (0606) .... 23
2.1.5.3 Users Are Allowed to Logon Without SNC (0593) ........ 23
2.1.5.4 Users - Other Than User Administrators - Are Authorized to Maintain the Mapping of SNC Users to SAP Users (0594) ......................... 24
2.1.5.5 SAP User IDs Have More Than One SNC User Attached (0595) .......... 24
2.1.6 Single Sign-On (SSO) Ticket .................................... 25
2.1.6.1 Unspecified Accepting of SSO Tickets (0603) .......... 25
2.1.6.2 Users - Other Than System Administrators - Are Authorized to Maintain the SSO Configuration (0604) ............................. 25

<Service Name>, <Customer Name> <date of session>
2.1.6.3 Users - Other Than System Administrators - Are Authorized to Maintain Trusted SSO Ticket Issuing Systems (0605) .......................................................... 26
2.1.6.4 Validity Period for the SSO Ticket Is Too Long (0607) .......................................................... 26
  2.1.6.4.1 Validity Period for the SSO Ticket Is Too Long (0607) 27
2.1.6.5 SSO Ticket Can Be Sent via an Unsecured Connection (0608) ............................................ 27
  2.1.6.5.1 SSO Ticket Can Be Sent via an Unsecured Connection (0608) 27
2.1.7 Certificate SSO .......................................................................................................................... 27
  2.1.7.1 External Authentication via Client Certificates (0621) .......................................................... 27
  2.1.7.2 Trusted Certification Authorities (0623) ................................................................................ 27
  2.1.7.3 Users - Other Than System Administrators - Are Authorized to Maintain Trusted CAs (0624) ........ 28
  2.1.7.4 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via SNC0 (0625) ................................................................. 28
  2.1.7.5 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via Table Maintenance (0626) .................................................. 29
  2.1.7.6 Users - Other Than User Administrators - Are Authorized to Maintain the Mapping of X.509 Users to SAP Users (0622) ...................................................... 29
2.1.8 Pluggable Authentication Services (PAS) ................................................................................ 30
  2.1.8.1 External Authentication via the Pluggable Authentication Services Is In Use (0631) .......... 30
  2.1.8.2 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via SNC0 (0633) ................................................................. 30
  2.1.8.3 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via Table Maintenance (0634) .................................................. 31
  2.1.8.4 Users - Other Than User Administrators - Are Authorized to Maintain the Mapping of External to SAP Users (0632) ...................................................... 31
3 SC_BASISADMIN - SECURITY CHECK BASIS ADMINISTRATION ............................................. 33
3.1 BASIS ADMINISTRATION AND BASIS AUTHORIZATIONS .................................................... 33
3.1.1 Basis Administration .................................................................................................................. 33
  3.1.1.1 Gateway and Message Server Security (SY084) ................................................................. 33
    3.1.1.1.1 Kernel Patch Level (SY086) .................................................................................................. 33
    3.1.1.1.2 Gateway Security (SY085) .................................................................................................. 33
      3.1.1.1.2.1 Gateway Security Properties (SY087) ............................................................................ 33
      3.1.1.1.2.2 Enabling an Initial Security Environment (SY088) ....................................................... 33
      3.1.1.1.2.3 Gateway Access Control Lists (SY089) ...................................................................... 33
    3.1.1.1.3 Message Server Security (SY091) .................................................................................... 34
      3.1.1.1.3.1 Separation of Internal and External Message Server Communication (SY092) ............ 34
      3.1.1.1.3.2 Message Server Administration Allowed for External Clients (SY093) ....................... 34
      3.1.1.1.3.3 Message Server Access Control List (SY094) ............................................................. 34
    3.1.1.2 Users - Other Than System Administrators - Are Authorized to Maintain System Profiles (0152) .................................................................................................... 34
    3.1.1.3 Users - Other Than System Administrators - Are Authorized to Start/Stop Application Servers (0154) ................................................................................................. 35
    3.1.1.4 Users - Other Than System Administrators - Are Authorized to Start/Stop Work processes (0156) ........................................................................................................... 35
    3.1.1.5 Users - Other Than System Administrators - Are Authorized to Lock/Unlock Transactions (0157) ............................................................................................................ 35
    3.1.1.6 Users - Other Than System Administrators - Are Authorized to Maintain Other User's Lock Entries (0159) ......................................................................................... 36
    3.1.1.7 Users - Other Than System Administrators - Are Authorized to Maintain Own Lock Entries (0166) ............................................................................................................ 36
    3.1.1.8 Users - Other Than System Administrators - Are Authorized to Delete or Reprocess Broken Updates (0161) ............................................................................................. 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.9</td>
<td>Users - Other Than System Administrators - Are Authorized to Activate a Trace (0163)</td>
</tr>
<tr>
<td>3.1.1.10</td>
<td>System Profiles Are Not Consistent (0153)</td>
</tr>
<tr>
<td>3.1.1.11</td>
<td>Table TPFDI Contains OS Passwords (0155)</td>
</tr>
<tr>
<td>3.1.1.12</td>
<td>No Critical Transactions Are Locked (0158)</td>
</tr>
<tr>
<td>3.1.1.13</td>
<td>No Timely Accurate Resolution of Erroneous Locks (0160)</td>
</tr>
<tr>
<td>3.1.1.14</td>
<td>No Timely Accurate Resolution of Broken Updates (0162)</td>
</tr>
<tr>
<td>3.1.1.15</td>
<td>Security Audit Log is not active (0170)</td>
</tr>
<tr>
<td>3.1.1.16</td>
<td>System Recommendations (ABAP) (SY123)</td>
</tr>
<tr>
<td>3.1.1.17</td>
<td>Sending Trace Data to Remote Client (0169)</td>
</tr>
<tr>
<td>3.1.1.18</td>
<td>Sending Trace Data to Remote Client (0169)</td>
</tr>
<tr>
<td>3.1.2.1</td>
<td>Batch Input No Timely Accurate Resolution of Failed Batch Input Sessions (0223)</td>
</tr>
<tr>
<td>3.1.2.2</td>
<td>Users - Other Than Batch Input Administrators - Are Authorized to Run Batch Input Sessions in Dialog (0221)</td>
</tr>
<tr>
<td>3.1.2.3</td>
<td>Users - Other Than Batch Input Administrators - Are Authorized to Administer Batch Input Sessions (0222)</td>
</tr>
<tr>
<td>3.1.3.1</td>
<td>Spool &amp; Printer Users - Other Than Spool Administrators - Are Authorized to Display Other Spool Requests (0192)</td>
</tr>
<tr>
<td>3.1.3.2</td>
<td>Users - Other Than Spool Administrators - Are Authorized to Display Protected Spool Requests of Other Users (0198)</td>
</tr>
<tr>
<td>3.1.3.3</td>
<td>Users - Other Than Spool Administrators - Are Authorized to Display the TempSe Content (0193)</td>
</tr>
<tr>
<td>3.1.3.4</td>
<td>Users - Other Than Spool Administrators - Are Authorized to Change the Owner of Spool Requests (0194)</td>
</tr>
<tr>
<td>3.1.3.5</td>
<td>Users - Other Than Spool Administrators - Are Authorized to Redirect a Print Request to Another Printer (0195)</td>
</tr>
<tr>
<td>3.1.3.6</td>
<td>Users - Other Than Spool Administrators - Are Authorized to Export a Print Request (0196)</td>
</tr>
<tr>
<td>3.1.3.7</td>
<td>Users - Other Than Spool Administrators - Are Authorized to Print on all Devices (0197)</td>
</tr>
<tr>
<td>3.1.4.1</td>
<td>Background Periodic Background Jobs Scheduled with User of Type Other Than 'SYSTEM' (0211)</td>
</tr>
<tr>
<td>3.1.4.2</td>
<td>Background Jobs That Are Not Used in Any Periodic Batch Job (0215)</td>
</tr>
<tr>
<td>3.1.4.3</td>
<td>Users - Other Than Background Administrators - Are Authorized to Schedule Jobs in SM36 (0212)</td>
</tr>
<tr>
<td>3.1.4.4</td>
<td>Users - Other Than Background Administrators - Are Authorized to Schedule Jobs in External Commands (0213)</td>
</tr>
<tr>
<td>3.1.4.5</td>
<td>Users - Other Than Background Administrators - Are Authorized to Schedule Jobs Under Another User Id (0214)</td>
</tr>
<tr>
<td>3.1.5.1</td>
<td>OS Access Users - Other Than System Administrators - Are Authorized to Define External OS Commands (0171)</td>
</tr>
<tr>
<td>3.1.5.2</td>
<td>Users - Other Than System Administrators - Are Authorized to Execute External OS Commands (0172)</td>
</tr>
<tr>
<td>3.1.5.3</td>
<td>Users - Other Than System Administrators - Are Authorized to View Content of OS Files with AL11 (0173)</td>
</tr>
<tr>
<td>3.1.6.1</td>
<td>Outgoing RFC Unsecured Outgoing RFC Calls (0252)</td>
</tr>
<tr>
<td>3.1.6.2</td>
<td>SNC Protection for encrypted outgoing RFC calls (0253)</td>
</tr>
<tr>
<td>3.1.6.3</td>
<td>Unexpected RFC Connections with Complete Logon Data Found (0254)</td>
</tr>
</tbody>
</table>
3.1.6.4 Users - Other Than System Administrators - Are Authorized to Administer RFC Connections (0255) .......................................................... 51
3.1.6.5 Users - Other Than System Administrators - Are Authorized to Access RFC Logon Information (0256) ......................................................... 52
3.1.6.6 Unexpected Trusting System Connections Found (0267) ......................................................... 52
3.1.6.7 Users - Other Than System Administrators - Are Authorized to Maintain Trusting Systems (0268) .......................................................... 52
3.1.6.8 Start of External Server Programs Is Not Restricted (0282) ......................................................... 53
3.1.6.9 Remote Monitoring Function for the RFC Gateway Is Not Disabled (0269) ............................... 53
3.1.6.10.1 Parameter gw/sim_mode <;GENERAL; Name> .......................................................... 54
3.1.7 Incoming RFC .......................................................... 54
3.1.7.1 Users Are Authorized to Run Any RFC Function (0241) ......................................................... 54
3.1.7.2 Users - other than Key Users - are Authorized to Visualize All Tables via RFC (0245) ............. 54
3.1.7.3 Incoming RFC with Expired Password is Allowed (0234) ......................................................... 55
3.1.7.4 Users authorized for Trusted RFC (Object S_RFCACL) (0239) ......................................................... 55
3.1.7.5 Users authorized for Trusted RFC which can be called from any calling user (0248) ............... 56
3.1.7.6 Unexpected Trusted System Connections Found (0238) ......................................................... 56
3.1.7.7 Users - Other Than System Administrators - Are Authorized to Maintain Trusted Systems (0240) .......................................................... 56
3.1.7.8 RFC Security in the Service Marketplace (0247) .......................................................... 57
3.1.8 Protection of Passwords in Database Connections (AB088) ......................................................... 57
3.1.9 Application Link Enabling (ALE) .......................................................... 57
3.1.9.1 Users - Other Than System Administrators - Allowed to Maintain the ALE Distribution Model (0723) ......................................................... 57
3.1.9.2 Users - Other Than System Administrators - Allowed to Maintain the Partner Profile (0724) .......................................................... 58
3.1.9.3 Do You Have any Additional Users with an Authorization to Receive IDOCs (0729) ............................... 58

4 SC_CHANGEMGMT - SC CHANGE MANAGEMENT ........................................................................ 60
4.1 CHANGE MANAGEMENT ........................................................................ 60
4.1.1 Data & Program Access ........................................................................ 60
4.1.1.1 Users - Other Than Key Users - Are Authorized to Start All Reports (0512) .......................... 60
4.1.1.2 Users - Other Than Key Users - Are Authorized to Display All Tables (0513) .................... 60
4.1.1.3 Users Are Authorized to Maintain All Tables (0514) .......................................................... 61
4.1.1.4 Users - Other Than System Administrators - Are Authorized to Change the Authorization Group of Tables (0515) .......................................................... 61
4.1.1.5 Users - Other Than Query Administrators - Are Authorized to Administer Queries (0517) .......................................................... 62
4.1.1.6 Users Are Authorized to Execute All Function Modules (0520) .......................................................... 62
4.1.2 Change Control ........................................................................ 63
4.1.2.1 System Change Option Not Appropriately Configured in the Production System (0301) ....... 63
4.1.2.2 Client Change Option Not Appropriately Configured (0302) .......................................................... 63
4.1.2.3 Users - Other Than System Administrators - Are Authorized to Change the System Change Option (0303) .......................................................... 64
4.1.2.4 Users - Other Than System Administrators - Are Authorized to Change the Client Change Option (0304) .......................................................... 65
4.1.2.5 Clients with an Entry in T000 but Without Any User Data (0319) .......................................................... 65
4.1.2.6 Users - Other Than System Administrators - Are Authorized to Create New Clients (0305) .......................................................... 66
4.1.2.7 Users Are Authorized to Delete Clients (0306) .............................................. 66
4.1.2.8 Users Are Authorized to Development in the Production System (0307) .............. 67
4.1.2.9 Users Are Authorized to Debug and Replace Field Values in the Production System (0308) .................................................................................................................. 67
4.1.2.10 Users Are Authorized to Perform Customizing in the Production System (0309) .... 68
4.1.2.11 Users Are Authorized to Develop Queries in the Production System (0310) .......... 68
4.1.2.12 Execution of CATTs and eCATTs Is Not Prevented by Client Settings (0311) ......... 69
4.1.2.13 Users Are Authorized to Execute CATTs in the Production System (0312) ........... 70
4.1.2.14 Users Are Authorized to Execute eCATTs in the Production System (0313) ......... 70
4.1.2.15 SAPgui User Scripting Is Enabled (0314) ................................................................. 71
4.1.2.16 Users Are Authorized to Use the Legacy Migration Workbench (0315) ................. 71
4.1.2.17 Table Logging Is Not Enabled Sufficiently (0316) ................................................ 72
4.1.2.18 Table Logging Is Not Enabled for Import (0317) .................................................. 72
4.1.2.19 Users Are Authorized to Modify the Table Logging Flag for Tables (0318) .......... 72
4.1.3 Development ........................................................................................................... 73
4.1.3.1 Development Sources Are Not Scanned for Critical Statements (0335) .......... 73
4.1.3.2 Development Keys Exist in the Productive System (0338) ........................................ 73
4.1.4 Transport Control .................................................................................................. 74
4.1.4.1 Users - Other Than Transport Administrators - Are Authorized to Change the TMS Configuration (0341) .................................................................................. 74
4.1.4.2 Users - Other Than Transport Administrators - Are Authorized to Start Imports to Production (0342) .................................................................................. 74
4.1.4.3 Users - Other Than Transport Administrators - Are Authorized to Create and Release Transports (0343) .................................................................................. 75
4.1.4.4 Users Are Authorized to Approve Transports (0346) ................................................ 75
4.1.4.5 Users - Other Than Transport Administrators - Are Authorized to Apply Patches (0363) ........................................................................................................ 76
4.1.4.6 Transports Are Not Scanned for Viruses (0348) ..................................................... 76
4.1.4.7 Program Versioning During Import is Not Enabled (0349) ........................................ 77
5 SC_USERAUTH - SC USER AUTHORIZATION CHECKS .............................................. 78
5.1 USER AUTHORIZATION .............................................................................................. 78
5.1.1 User Management .................................................................................................. 78
5.1.1.1 Users - Other Than the User Administrators - Are Authorized to Maintain Users (0002) ........................................................................................................ 78
5.1.1.2 User Administrators Are Authorized to Change Their Own UserMaster Record (0003) ........................................................................................................ 78
5.1.1.3 User Administrators Are Allowed to Maintain Users of Any Group (0004) .......... 79
5.1.1.4 Users Are Not Assigned to User Groups (0005) ...................................................... 79
5.1.1.5 User Data Is Incomplete (0006) ............................................................................. 80
5.1.1.6 User Master Data Is Not Regularly Synchronized with a Corporate LDAP Directory (0007) ........................................................................................... 80
5.1.1.7 Users with Authorizations for User and Role/Profile/Authorization Maintenance (0008) ........................................................................................... 80
5.1.1.8 Reference Users Are Used (0011) ........................................................................... 81
5.1.1.9 Usage of 'Normal' Users as Reference Users Is Not Prohibited (0012) ................... 81
5.1.1.10 Users - Other Than User Administrators - Are Authorized to Access Tables with User Data (0013) .................................................................................. 81
5.1.1.11 Users - Other Than User Administrators - Are Authorized to Call Function Modules for User Admin (0019) .................................................. 82
5.1.2 Super Users ............................................................................................................. 83
5.1.2.1 Users Have Nearly All Authorizations (0023) ......................................................... 83
5.1.2.2 Unexpected Users Are Authorized to Change a Super User Accounts (0026) .......... 83
5.1.2.3 Users with the most Full Access Authorizations (* Field Values) (0027) ................. 83
5.1.3.1 User SAP* has the default password in some clients (0041).................. 85
5.1.3.2 Not all profiles are removed from user SAP* (0042) ......................... 85
5.1.3.3 User SAP* is neither locked nor expired (0043) .......................... 85
5.1.3.4 User SAP* is not assigned to the user group SUPER (0044) ........... 85
5.1.3.5 User SAP* has been deleted at least in one client (0045) .............. 86
5.1.3.6 Usage of the hard coded user SAP* is not disabled (0046) .............. 86
5.1.3.6.1 Usage of the hard coded user SAP* is not disabled (0046) ........... 86
5.1.3.7 User SAP*’s activities are not logged in the Security Audit Log (0047) ... 86
5.1.3.8 User DDIC has the default password in some clients (0048) .............. 87
5.1.3.9 User DDIC Is Not Assigned to the User Group SUPER (0049) .......... 87
5.1.3.10 User DDIC’s activities are not logged in the Security Audit Log (0050) .. 87
5.1.3.11 User SAPCPIC has the default password in some clients (0051) ....... 88
5.1.3.12 User SAPCPIC Is Neither Locked nor Expired (0052) .................. 88
5.1.3.13 User SAPCPIC Not Assigned to the Group SUPER (0053) ............. 88
5.1.3.14 User SAPCPIC Has More Authorizations Than Required (0054) ...... 89
5.1.3.15 User SAPCPIC’s activities are not logged in the Security Audit Log (0055) 89
5.1.3.16 User EARLYWATCH has the default password (0056) .................. 89
5.1.3.17 User EARLYWATCH Is Not Assigned to User Group SUPER (0058) .... 89
5.1.3.18 User EARLYWATCH Has More Authorizations Than Required (0059) ... 90
5.1.3.19 User EARLYWATCH’s activities are not logged in the Security Audit Log (0060) ... 90
5.1.3.20 User TMSADM has the default password in some clients (0063) ....... 90
5.1.3.21 User TMSADM Exists in Clients Other Than Client 000 (0064) ........ 91
5.1.3.22 User TMSADM has more authorizations than required (0065) ......... 91
5.1.4 Role & Authorization Management ................................................. 91
5.1.4.1 Users Are Authorized to Maintain Roles Directly in the Production System (0072) ... 91
5.1.4.2 Users Are Authorized to Maintain Profiles Directly in the Production System (0073) 92
5.1.4.3 Users Are Authorized to Maintain Authorizations Directly in the Production System (0074) .......................................................... 92
5.1.4.4 Users Are Authorized to Call Function Modules for Authorization, Role and Profile Management (0087) .............................................. 93
5.1.4.5 SAP Standard Roles Are Assigned to Users (0082) ......................... 93
5.1.4.6 SAP Standard Profiles Are Assigned to Users (0083) ..................... 94
5.1.4.7 Inconsistent Assignment of Generated Profiles (0084) ................. 94
5.1.4.8 Unused Roles Are Found (0086) .................................................. 94
5.1.4.9 Profiles on Long Time Locked Users (0089) .................................. 95
5.1.5 Authorizations .................................................................................. 95
5.1.5.1 Authorization Checks Within Certain Transactions Are Partly Disabled (0101) ....... 95
5.1.5.2 Authorization Checks for Certain Authorization Objects Are Disabled (0103) ....... 95
5.1.5.3 Users Are Authorized to Disable Authorization Checks Within Transactions (0102) ........ 96
5.1.5.4 Users Are Authorized to Disable Authorization Checks Globally (0105) .......... 96
5.1.5.5 Users Are Authorized to Call Any Transaction (0110) ..................... 96
5.1.5.6 Users Are Authorized to Delete an Authorization Check Before Transaction Start (0111) ............................ 97
5.1.5.7 Global Disabling of Authority Checks Is Not Prevented (0104) ........ 97
5.1.5.8 Authority Check for Inbound RFC Connections Is Disabled (0106) ........ 98
5.1.5.8.1 Authority Check for Inbound RFC Connections Is Disabled (0106) ........ 98
5.1.5.9 Authority Check for Inbound tRFC Connections Is Disabled (0107) ....... 98
5.1.5.10 Authority Check for Particular ABAP Elements Is Disabled (0108) ........ 99
5.1.5.11 Authority Check on S_TCODE Is Disabled (0109) .......................... 99
5.1.5.12 Users Comparison After Role Change Is Not Run in a Timely Accurate Manner (0112) .............................................................. 99
5.1.5.12.1 Users Comparison After Role Change Is Not Run in a Timely Accurate Manner (0112) ......................................................... 100

6 SC_WEBAS - WEB APPLICATION SERVER ................................................................. 101
6.1 WEB APPLICATION SERVER .................................................................................. 101
6.1.1 Internet Communication Framework (ICF) .......................................................... 101
6.1.1.1 Active ICF Services (0664) .............................................................................. 101
6.1.1.2 Unused ICF Services Are Activated (0652) ....................................................... 101
6.1.1.3 ICF Service Can Be Called via Unsecured http Connection (0653) ............... 101
6.1.1.4 Access to ICF Services Does Not Require Authorization for S_SICF (0654) .... 102
6.1.1.5 Users - Other Than System Administrators - Are Authorized to Activate ICF Services (0655) .................................................. 102
6.1.1.6 Users - Other Than System Administrators - Are Authorized to Access Table Authorization Group &NC& (0663) ......................... 102
6.1.1.7 External Clients Are Allowed to Switch the Profile Level (0702) ......................... 103
6.1.1.7.1 External Clients Are Allowed to Switch the Profile Level (0702) ............... 103
6.1.2 http Client .......................................................................................................... 103
6.1.2.1 Additional http Client Connections Found (0682) .......................................... 103
6.1.2.2 No Proxy Used to Connect to http Servers (0683) ........................................... 104
6.1.2.3 No Authorization for S_SICF Required for http Client Access (0684) ............. 104
6.1.2.4 Client Proxy Does Not Require Client Authentication (0685) ......................... 104
6.1.2.5 Additional http Connections with Full Logon Data Found (0687) ..................... 105
6.1.2.6 No Encryption of Outgoing http Communication (0688) ............................... 105
6.1.3 Internet Communication Manager (ICM) ............................................................ 105
6.1.3.1 Users - Other Than System Administrators - Are Authorized to Administer the ICM (0701) ...................................................... 105
6.1.3.2 Users - Other Than System Administrators - Are Authorized to Display the http Server Cache (0705) ........................................ 106
6.1.3.3 Users - Other Than System Administrators - Are Authorized to Configure the ICM Monitor (0706) ......................................................... 106
6.1.3.4 External Clients Are Allowed to Switch the Trace Level (0703) ....................... 107
6.1.3.4.1 External Clients Are Allowed to Switch the Trace Level (0703) ................. 107
6.1.3.5 ICM (Internet Communication Manager) Is Active (0704) .............................. 107
6.1.3.5.1 ICM (Internet Communication Manager) Is Active (0704) ....................... 107
6.1.3.6 Not all http Service Requests Are Logged (0662) .......................................... 107
6.1.4 PSE Management ................................................................................................. 108
6.1.4.1 Users - Other Than System Administrators - Are Authorized to Maintain the System PSE's (0711) ........................................ 108
6.1.5 J2EE - Backend Checks (Dual Stack System) ....................................................... 108
6.1.5.1 Users with Role "SAP_J2EE_ADMIN" (0813) ..................................................... 108
6.1.5.2 Guest user should be locked (J135) ................................................................. 109
6.1.5.3 Guest User should be locked (J136) ............................................................... 109
6.1.5.4 Profile of User SAPJSF (0796) ................................................................... 110
6.1.5.5 Type of Users in the Jco RFC Provider (0877) ................................................. 110
6.1.5.6 Authorization of Users in the Jco RFC Provider (0878) ................................. 111
6.1.5.7 J2EE Engines Allowed to Access the Application Server (0881) .................... 112
6.1.5.8 Other J2EE Systems Allowed to Connect to the SAP Database for User Replication (0863) ...................................................... 113
6.1.5.9 Users Authorized to Maintain the Sending Systems for User Replication (0864) 113

7 SC_HR - SC HUMAN RESOURCES MODUL ................................................................... 115
7.1 HUMAN RESOURCES ............................................................................................. 115
7.1.1 Human Resources General Checks............................................................................. 115
  7.1.1.1 Users - Other Than HR Administrators - Are Authorized to Maintain Table T77S0 (0922) .................................................................................................................. 115
  7.1.1.2 Users - Other Than HR Administrators - Are Authorized to Maintain Tables for Organizational Data (0923) ...................................................................................... 115
  7.1.1.3 Users - Other Than HR Administrators - Are Authorized to Read the Infotype Change Log (0924) .............................................................................................................. 116
  7.1.1.4 Users - Other Than HR Administrators - Are Authorized to Read HR Tables with Person Related Data (0925) .................................................................................................. 116
  7.1.1.5 Users - Other Than HR Administrators - Are Authorized to Change HR Tables with Person Related Data (0926) .................................................................................. 117
  7.1.1.6 Users - Other Than HR Administrators - Are Authorized to Maintain Client Dependant HR Customizing (0927) ..................................................................................................... 117
  7.1.1.7 Users - Other Than HR Administrators - Are Authorized to RunAll HR Transactions (0928) ............................................................................................................................ 118
  7.1.1.8 Users - Other Than HR Administrators - Have Broad Authorization on HR Reports (0929) ................................................................................................................................. 118

7.1.2 Personal Administration .............................................................................................. 118
  7.1.2.1 Users - Other Than HR Administrators - Are Authorized to Read HR Master Data (0936) ............................................................................................................................... 118
  7.1.2.2 Users - Other Than HR Administrators - Are Authorized to Change Master Data without Double Verification (0937) ..................................................................................... 119
  7.1.2.3 Users - Other Than HR Administrators - Are Authorized to Delete Personnel Numbers (0938) .................................................................................................................. 119
  7.1.2.4 Users - Other Than HR Administrators - Are Authorized to Change their Own Master Data (0939) ................................................................................................................. 120

7.1.3 Payroll ......................................................................................................................... 120
  7.1.3.1 Users - Other Than HR Administrators - Are Authorized to Read Payroll Results (0946) ................................................................................................................................. 120
  7.1.3.2 Users - Other Than HR Administrators - Are Authorized to Maintain Personell Calculation Schemas (0947) ............................................................................................. 121
  7.1.3.3 Users - Other Than HR Administrators - Are Authorized to Release a Payroll Run (0950) ........................................................................................................................... 121
  7.1.3.4 Users - Other Than HR Administrators - Are Authorized to Delete Payroll Results (0951) ............................................................................................................................... 122

8 SC_CUSTOMERCHECKS - GROUP FOR CUSTOMER SPECIFIC CHECKS .................. 123
  8.1 CUSTOMER SPECIFIC AUTHORIZATION CHECKS .................................................. 123
    8.1.1 <;GENERAL;KeyfigName> ..................................................................................... 123
  8.2 CUSTOMER DEFINED AUTHORIZATION CHECKS .................................................. 123
    8.2.1 <;GENERAL;KeyfigName> ..................................................................................... 124

9 SC_SAPROUTER - CHECKS FOR THE SAPROUTER .................................................. 126
  9.1 SAPROUTER ............................................................................................................... 126
    9.1.1 No Encryption (SNC or VPN) Used for the Connection to SAP (0541) ............... 127
    9.1.2 Non SNC-protected Communication from the Internet Allowed in the Saprouterab (0542) ........................................................................................................................ 128
    9.1.3 SAPRouter Allows General Access to All Customers SAP Systems from Everywhere (0543) ...................................................................................................................... 129
    9.1.4 SAPRouter Allows Generic Communication Partners (Incoming) ?(0544) ............ 129
    9.1.5 SAPRouter Allows Generic Access to the Customers Servers (0545) .................... 130
    9.1.6 Destination Service for SAProuter is Not Fully Qualified and Contains the Asterix (0546) ......................................................................................................................... 131
9.1.7 SAProuter Allows Permanent OS Access (0548) ...................................................... 132
9.1.8 Access from SAP via the SAProuter Doesn't Require SAProuterPassword (0553) 132
9.1.9 SAProuter Connections Are Not Logged (0554)...................................................... 133
9.1.10 Activities of the OSS Users Are Not Logged in the Security Audit Log (0533) .. 133
1 SC_INIT - Initializations for Security Check

1.0.1 Preface
The SAP Security Optimization service is a comprehensive support service that identifies security risks for your SAP system and helps you to determine the appropriate measures to protect it from these risks.

Objective of the SAP Security Optimization Service
The objectives of SAP Security Optimization are:
- To analyze the technical configuration of your SAP system for security risks
- To provide recommendations for implementing measures to mitigate security risks
- To provide a compressed overview of the implemented security level
- To enable you to protect your business systems from typical security risks

The security checks of SAP Security Optimization are performed for the following security aspects:
- **Availability**: ensuring that a system is operational and functional at any given moment
- **Integrity**: ensuring that data is valid and cannot be compromised
- **Authenticity**: ensuring that users are who they claim to be
- **Confidentiality**: ensuring that information is not accessed by unauthorized persons
- **Compliance**: ensuring that the system security setup is in accordance with established guidelines

Scope of SAP Security Optimization
SAP Security Optimization includes a collection of several hundred checks. These checks identify security vulnerabilities in the current setup and configuration of your SAP system. The checks are performed on the SAP software layer. For a security analysis of the underlying operating system and database, consult your vendor; for a security analysis of the network, contact your preferred network security provider.

The SAP Security Optimization service cannot cover customer-specific aspects that require a detailed on-site analysis, such as the following checks:
- Segregation of duties for business-critical processes
- Security organization (organizational security)
- Security administration processes (operational security)

For a complete overview of existing security risks to your business system, the topics listed above have to be taken into consideration. SAP's Security Consulting Team can assist you with individual on-site consulting services to obtain guidance on aspects of security.

1.1 Detected Issues

Purpose
This action list is created automatically from all checks whose rating is RED. If necessary, you can add more information to the generated list.

Procedure
Add as many rows as you like. They always appear at the top of the list.

Important: If you open this check before all checks have been rated, the additional checks you rate later will not appear in the list until you initialize this check again.

Risk Rating
No rating: "To Do/Done" list
The following list gives you an overview of all checks in the SAP Security Optimization service that are rated with a high risk:
Recommendation: Look at the list of the action items above very carefully and decide if anything on this list needs to be adjusted in your environment. First, read the complete report, and then decide for each check whether it is advisable for you to change the current situation. Sometimes you will find out that your current situation is sufficient, even if checks are rated with a medium or even high risk. Since every SAP implementation is different, you have to adjust this general report to your particular situation.

1.2 Special Focus Checks

1.2.1 Compare Clients From Download to Questionnaire Data

**Purpose**
To warn the customer if there are unchecked clients in the system.

**Procedure**
Compare the downloaded clients from ST14 with the clients from the questionnaire.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: No unchecked clients.
- **YELLOW/RED**: Unchecked clients.
- **RED**: The following clients in your system have not been checked.
- **YELLOW**: The following clients in your system have not been checked.

1.2.2 Client Overview

**YELLOW**: Clients that are not analyzed are highlighted in yellow.
For several key figures, the analysis is restricted to the clients specified in the questionnaire.
Recommendation: Review the list and check whether the analyzed clients fulfill your needs.
The following table lists clients that are available in the analyzed system and clients that have been specified in the questionnaire for analysis.

1.2.3 Additional Super User Accounts Found (0022)

**Purpose**
To identify users with more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found (except those specified in the questionnaire) who have surplus authorizations.
- **YELLOW/RED**: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.
- **RED**: Evaluated Risk - High

In this system, the following superuser accounts were found that were not mentioned in the questionnaire. (These are the users having the profile SAP_ALL).
All superuser accounts that were found in your system are REMOVED from all the following checks. This means that checks that report 5 authorized users, for example, actually have 5 users and ALL superuser accounts authorized for your system. Keep this in mind when you look at all other checks below.
Recommendation:
Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

1.2.4 Users - Other Than System Administrators - Are Allowed to Call ST14 (0168)

**Purpose**
To identify users with more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found (except those specified in the questionnaire) who have surplus authorizations.
- **YELLOW/RED**: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.
- **RED**: Evaluated Risk - High

The download for the SAP Security Optimization can be viewed by any user who has authorization for transaction ST14. For this reason, this authorization is very critical and should only be given to very limited users. The SAP Security Optimization data is sensitive, it contains the current security situation for your SAP system. If this information falls in the wrong hands, there is a potential for major security issues.

**Recommendation:**
Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD=ST14 [and all relevant parameter transactions]
2 SC_AUTHENTICATION - SC Authentication checks

2.1 Authentication

2.1.1 Password Logon Is at Least Partly Allowed (0139)

Purpose
To check whether users can log on to the instance only by means of single sign-on (SSO) or strong authentication.

Procedure
The profile parameters login/disable_password_logon and login/password_logon_usergroup are checked for each application server. If at least a few users are able to logon with passwords, this check is shown.

Risk Rating
No risk rating.

YELLOW:
Logging on with passwords is at least partially allowed. Allow all users to log on with their password (login/disable_password_logon = 0), or at least special groups that are described in the parameter login/password_logon_usergroup.

Recommendation:
If you are not using Single Sign-On (SSO), at least think about implementing an SSO solution. To further increase the security of your systems, prevent users from logging on with their passwords.

2.1.2 Password Policy

If password login is allowed for specific instances only, the password policy is checked only for these instances.

2.1.2.1 Password Complexity

2.1.2.1.1 Minimum Password Length (0126)

RED:
Evaluated Risk - High
The current system settings allow a password length less than 6 characters. This allows weak passwords. Attackers may successfully recover these passwords and gain unauthorized access to the system.

YELLOW:
Evaluated Risk - Medium
The current system settings allow a password length of less than 8 characters. This allows weak passwords. Attackers may successfully recover these passwords and gain unauthorized access to the system.

GREEN:
The current system settings do not allow password logon, or the minimum password length is at least 8 characters on all instances.

Recommendation: Assign a minimum value of 8 to the profile parameter login/min_password_lng.

2.1.2.1.2 Character Category Settings (AU093)

Evaluated Risk - Medium
Information
SAP provides options to enforce complex passwords. Find the current settings of the corresponding profile parameters in the table.
Recommendation: Enforce a minimum of 3 independent character categories using the corresponding profile parameters. For more information, see SAP Note 862989 and the section Profile Parameters for Logon and Password (Login Parameters), on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

2.1.2.1.3 Trivial Passwords Are Not Sufficiently Prohibited (0125)

Purpose
To check whether the customer attempts to prevent passwords from being guessed by filling table USR40. If this table is filled, users are no longer allowed to use passwords in this table. The more entries in this table the better.

Procedure
The system counts the number of entries in table USR40.

Risk Rating
The rating is done automatically as follows:
Green: 100 or more entries are in table USR40.
Yellow: 1-99 entries are in table USR40.
Red: No entries are in table USR40.

Evaluated Risk - High
No entries are maintained in table USR40. This table is used for preventing passwords from being guessed easily. In this table you could exclude your company name, your town, your products, and so on. You can use the wildcard (**) for generic entries.

Recommendation:
Maintain at least 100 values in table USR40.

Evaluated Risk - Medium
You already use entries in table USR40. They can be used on a generic level as well.

Recommendation:
Maintain at least 100 values in table USR40 to prevent passwords from being guessed easily.

2.1.2.2 Initial Passwords

2.1.2.2.1 Validity of Initial Passwords

RED:
There is no time restriction on the validity of initial passwords.

YELLOW:
Initial passwords are valid for more than 14 days.

Recommendation: Proceed as follows:
- Handle users of type C (Communication) with initial passwords because they will be locked if the above profile parameter is set.
Use transaction SUIM/report RSUSR200 in each client to find users of type C (Communication).
If these users are active and in use, switch the user type to B (System). This has no negative effect.
- Restrict the password validity to 14 days or less. Note that the value 0 grants unlimited validity.
- For more information, see SAP Note 862989 and the Profile Parameters for Logon and Password (Login Parameters) section, either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.
2.1.2.2 Users with Initial Passwords Who Have Never Logged On (0009)

**Purpose**
To check whether a large group of users still has initial passwords. This is especially critical if mostly the same initial passwords are used, because then other users could log on instead.

**Procedure**
The system looks for users who have never logged on to the system. This can also be checked by using report RSUSR200.

**Risk Rating**
The rating is done automatically as follows:
- **Green:** Less than 5% of the users have initial passwords.
- **Yellow:** 5%-9% of the users have initial passwords.
- **Red:** At least 10% of the users have initial passwords.

**Recommended Action:**
Check why so many users have initial passwords. Ask these users to change their passwords using the profile parameter login/password_change_for_SSO, for example. Or delete these users if they do not need access to the SAP system.

You can use report RSUSR200 of the User Information System (transaction SUIM) to identify users with initial passwords.

2.1.2.3 Users with Reset Password Who Have Not Logged On (0140)

**Purpose**
To check whether a large group of users still has passwords that have been reset. This is especially critical if the passwords are reset to "well-known" passwords, because then other users could log on instead.

**Procedure**
The system looks for users who have never logged on. This can also be checked by report RSUSR200.

**Risk Rating**
The rating is done automatically as follows:
- **Green:** Less than 5% of the users have passwords that have been reset.
- **Yellow:** 5%-9% of the users have passwords that have been reset.
- **Red:** At least 10% of the users have passwords that have been reset.

**Recommended Action:**
Check why so many users have passwords that have been reset. Ask them to change their passwords with, for example profile parameter login/password_change_for_SSO. Or delete these users if they do not need access to the SAP system.

2.1.2.3 Interval for Logon with Productive Password Is Too Long (AU081)

**Purpose**
To check whether the system automatically invalidates unchanged productive passwords (a password chosen by the user) after n days.

**Procedure**
The system checks the profile parameter login/password_max_idle_productive. The return value is the validity period of a productive password in days.

**Risk Rating**

The rating is assigned automatically as follows:

**GREEN:** The parameter is set to 1 or greater.
**YELLOW:** The parameter is set to 0 (disabled).

**Background:**

Profile Parameters for Logon and Password (Login Parameters)

`login/password_max_idle_productive;`

Specifies the maximum period for which a productive password (a password chosen by the user) remains valid if it is not used. After this period has expired, the password can no longer be used for authentication purposes. The user administrator can reactivate password-based logon by assigning a new initial password.

Permissible values: 0 – 24,000 (unit: days); Default value 0, that is, the check is deactivated

Available as of SAP NetWeaver 7.00

**YELLOW:**

**Recommendation:** Activate profile parameter `login/password_max_idle_productive`.

This parameter specifies the maximum period for which a productive password (a password chosen by the user) remains valid if it is not used. After this period has expired, the password can no longer be used for authentication purposes.

For more information, see:

SAP Note 327917 - New user types as of Release 4.6C
SAP Note 862989 - New password rules as of SAP NetWeaver 2004s (NW ABAP 7.0)
Online Help – Profile Parameters for Logon and Password (Login Parameters)

**Evaluated Risk - Medium**

As of SAP NetWeaver 7.00, SAP supports this parameter to encourage your users to create more secure passwords.

**2.1.2.3.1 login/password_max_idle_productive**

**2.1.2.4 Interval for Password Change Is Too Long (0127)**

**Purpose**

To check whether users have to change their passwords on a regular basis.

**Procedure**

The system checks the profile parameter `login/password_expiration_time`. The return value is the password validity in days.

**Risk Rating**

The rating is done automatically as follows:

**Green:** The parameter is set to values lower than or equal to 60, but not 0.
**Yellow:** The parameter is set to 61-120.
**Red:** The parameter is set to 0, or to values higher than 120.

**RED:**

**Evaluated Risk - High**

You are currently using a password change interval of more than 120, or you have deactivated this option completely.

Recommendation: Change the profile parameter `login/password_expiration_time` to 30 (or at least not higher than 60, and definitely not to 0 (disabled)).

**YELLOW:**

**Evaluated Risk - Medium**

You are currently using a password change interval of 61 to 120 days. This is quite a long period of time.

Recommendation: Change the profile parameter `login/password_expiration_time` to 30 (but not higher than 60 and definitely not to 0 (disabled)).
2.1.2.5 Too Many Invalid Logon Attempts Allowed Before a Session Is Terminated (0132)

Purpose
To check the number of failed logon attempts before the session is terminated.

Procedure
The system checks the profile parameter login/fails_to_session_end. The return value is the number of failed logon attempts before the session is terminated.

Risk Rating
The rating is done automatically as follows:
Green: The value is set between 1 and 3.
Yellow: The value is set to more than 3, or to 0, which disables this value.

Evaluated Risk - Medium
You have set the profile parameter login/fails_to_session_end to '0' (disable) or to values larger than 3.
Recommendation: As this parameter controls the number of failed logon attempts before the sessions ends, we recommend that you set this value between 1 and 3.

2.1.2.6 Too Many Incorrect Logon Attempts Allowed Before a User Is Locked (0133)

Purpose
To check the number of failed logons before a user is locked.

Procedure
The system checks the profile parameter login/fails_to_user_lock. The return value is the number of failed logons before a user is locked.

Risk Rating
The rating is done automatically as follows:
Green: The parameter is lower than 7.
Red: The parameter is 7 or higher.

Evaluated Risk - High
You are allowing more than 6 logon attempts with a wrong password before the user is locked. This is an extremely high number if attackers are trying to guess the password.
Recommendation: Reduce the profile parameter to 6 or lower to increase security.

2.1.2.7 User Locks due to Failed Logon Attempts Are Automatically Released at Midnight (0134)

Purpose
To check whether the system automatically unlocks users at midnight.

Procedure
The system checks the profile parameter login/failed_user_auto_unlock. The return value '1' means automatic unlocking, and the return value '0' means no automatic unlocking at midnight.

Risk Rating
The rating is done automatically as follows:
Green: Automatic unlocking is disabled (return value '0').
Red: Automatic unlocking is enabled (return value '1').

Evaluated Risk - High
Currently all your locked accounts are automatically unlocked at midnight. This is very risky because you are not able to detect password attacks for special users at that time.
Recommendation: Set this parameter to 0, which means that all locked users have to be unlocked by an administrator. In this way, the administrator can look specifically for password attacks.
2.1.2.8 Security Attack Indicated by Users Locked due to Incorrect Logon Attempts (0141)

**Purpose**
To check whether the customer is hit by an undetected password attack on users who rarely use the system.

**Procedure**
The system checks the percentage of users that are locked because of incorrect logon attempts. If SAP* or DDIC are contained in the results list, this is a lot more critical than for any other user. Report RSUSR300 can also be used for this purpose.

**Risk Rating**
The rating is done automatically as follows:
GREEN: SAP* and DDIC are not locked because of incorrect logon attempts and the total percentage is below 5% in all clients.
YELLOW: Either SAP* or DDIC is locked because of incorrect logon attempts, or at least 5% of the users are locked for the same reason in at least one client.

**Evaluated Risk - Medium**
SAP* or DDIC users are locked because of incorrect logon attempts or at least 5% of your users are locked in one client.

Recommendation:
Check who is causing these incorrect logon attempts to attack your system or who cannot remember their password.

2.1.3 General Authentication

2.1.3.1 Users Who Have Not Logged On for an Extended Period of Time (0010)

**Purpose**
To find users who have not logged on to the system for more than 90 days.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check. Compare the TRDAT field in table USR02 with the current date.

**Risk Rating**
The rating is set automatically as follows:
GREEN: No users found.
YELLOW: There are users that have not logged on to the system for more than 90 days but have valid user accounts.

**Evaluated Risk - Medium**
Recommendation:
A large number of users have not logged on to the SAP system in the last 2 months. Determine the reason for this. Either there are users registered in the SAP system who never use the system, or there are users in your system who are no longer in your company. Since the SAP license is user-based, we recommend that you check this and either delete or lock some of the users. You can use report RSUSR200 of the User Information System (transaction SUIM) to identity users with initial passwords.

2.1.3.2 Security Critical Events for End Users Are Not Logged in the Security Audit Log (0136)

**YELLOW:**
**Evaluated Risk - Medium**
Recommendation:
Use transaction SM19 to activate logging of failed logon attempts for all your users in all clients. It is then possible to find out who performed which action, and how to detect an unauthorized logon attempt.
2.1.3.3 Interval After Which Inactive Users AreLogged Off Is Too Long (0137)

**Purpose**
To check whether a user is automatically logged off after a certain time of inactivity.

**Procedure**
The system checks the profile parameter rdisp/gui_auto_logout. The return value is the elapsed time in seconds before a user is logged off automatically.

**Risk Rating**
The rating is set automatically.

- **GREEN:** The value is between 1 and 3600.
- **YELLOW:** The value is 0 or higher than 3600.

**Background**
Prohibits misuse of unwatched PC without password-protected screen saver.

- **YELLOW:**

**Evaluated Risk - Medium**
If you deactivate this parameter by setting it to '0' or if you use a value higher than 1 hour, it is likely that users who are no longer in the office remain logged on. If you do not use screen savers at all workstations, this could result in other users accessing these workstations to get to unauthorized information.

Recommendation: Set this value to 1800 or 3600, for example, to reduce this risk as far as possible. Also, do not automatically log off users who have been idle for only a few minutes.

2.1.3.4 Multiple Logons Using the Same User ID Is Not Prevented (0138)

**Purpose**
Checks whether multiple logons with a single user account are possible (sharing user accounts).

**Procedure**
The system checks the profile parameter login/disable_multi_gui_login. The return value is '0' if the multiple logons are allowed, and '1' if this option is disabled.

**Rating**
The check is not rated. It is only shown if the value is set to 0.

**Background**
Sharing of user accounts does not allow you to trace security violations, and might result in users having too many authorizations.

- **YELLOW:**

**Evaluated Risk - Medium**
Sharing user accounts does not allow you to trace security violations and may result in users having too many authorizations.

Recommendation: Set this value to '1' so that each user has to log on with a different account.

2.1.3.5 Users - Other Than User Administrators - Are Authorized to Change Passwords (0121)

**Purpose**
Find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

- **Green:** No users found (except those specified in the questionnaire) who have surplus authorizations
- **Yellow/Red:** Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - High**
The following users are allowed to change and reset passwords. This is very risky because all these users could change the password and log on themselves with any user. The only
consequence is that the "real user" would no longer be able to log on, because the password has been changed. This results in the password being reset because there is a chance that the "real user" might think they have forgotten the correct password.

Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SU01 or TCD=OIBB or TCD=OOUS or TCD=OPF0 or TCD=OPJ0 or TCD=OVZ5 [as well as all relevant parameter transactions]
Object 2: S_USER_GRP with ACTVT=05

2.1.3.6 Users - Other Than User Administrators - Are Authorized to Lock/Unlock Users (0135)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

Green: No users found (except those specified in the questionnaire) who have surplus authorizations

Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

RED:
Evaluated Risk - High
Unauthorized system access because it is possible to unlock any user. In addition, interfaces may malfunction which results in the connected user being locked.

Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SU01 or TCD=OIBB or TCD=OOUS or TCD=OPF0 or TCD=OPJ0 or TCD=OVZ5 [as well as all relevant parameter transactions]
Object 2: S_USER_GRP with ACTVT=05

2.1.4 Password Based Authentication Admits Password Attacks (0591)

Purpose
SNC-enabling activates new tables such as the USRACL table. We inform the customer of this in this check. This check is used to activate several more SNC checks, if SNC is enabled.

Procedure
Check in the download module whether the profile parameter snc/enable = 1 and whether you can find at least one entry with an SNC name maintained in the USRACL table.

Risk Rating
No rating. We inform the customer if SNC authentication is enabled for SAP GUI users.

YELLOW:
You have deactivated SNC (snc/enable=0) or at least do not use it for the authentication of SAP GUI users since there are no SNC entries in the table USRACL.
SNC enables external authentication and therefore allows a higher security level for your system (by using smart cards with user credentials, for example). Since your system allows password authentication, a password attack is still possible (although you can minimize this risk by enforcing a password policy).

2.1.5 SAP GUI Single Sign-On (SSO)

2.1.5.1 Password Logon Is Allowed to SNC Enabled Servers (0592)

Purpose
The system checks whether the password logon is allowed for servers that use SNC. As Single-Sign On (SSO) is activated, we recommend that you use it. The use of SSO increases security.

Procedure
The system checks the setting of the profile parameter snc/accept_insecure_gui.

Risk Rating
The rating is done automatically as follows:
- Green: The parameter value is set to '0'.
- Red: The parameter value is '1' or 'U'.
- YELLOW: You are still allowing access to the system without SSO, even though you have enabled SNC on the server. This means that passwords are still vulnerable to attack.

Recommendation: Check whether it is really necessary to allow authentication by means of passwords. At least change this parameter to '0' for general purposes, and to '1' (or, even better, to 'U') on the central instance for administration purposes.

2.1.5.2 SNC Users Do Not Have to Change Their Initial Password (0606)

Purpose
Are users who use Single Sign On (SSO) to log on to the system allowed to change their initial password? If not, this results in many initial passwords for many users who would normally use SSO because they forget to change the initial password.

Procedure
The system checks the setting of the profile parameter login/password_change_for_SSO.

Risk Rating
The rating is done automatically as follows:
- GREEN: The parameter value is set to 1.
- RED: The parameter value is either 0.

Evaluated Risk - High
You use SNC, but you do not enforce that all the initial passwords are changed at least once when users log on for the first time.

Recommendation:
Set the parameter login/password_change_for_SSO to 1. Only then can you ensure that users no longer have initial passwords in systems with SSO usage.

2.1.5.3 Users Are Allowed to Logon Without SNC (0593)

Purpose
To check in a system that is SNC-enabled, which users can log on without using SNC. Since they can then log on with their password, this number must be limited to reduce the risk. The customer must be aware of the specific users who have this setting. For this reason, all users are displayed who are allowed to log on with a password.

Procedure
The system checks the field GUIFLAG in table USRACL. If this field is set to 'X', this user is allowed to log on with a password, while the system sets the profile parameter snc/accept_insecure_gui to 'U'.
Risk Rating
This check is not rated. It is for information purposes only.
YELLOW:
The users listed above are still allowed to log on to the system with their password instead of using SSO. You should be aware of this.

Recommendation:
Reduce the number of users who are allowed to log on with their password to the absolute minimum.

2.1.5.4 Users - Other Than User Administrators - Are Authorized to Maintain the Mapping of SNC Users to SAP Users (0594)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

Green: No users found (except those specified in the questionnaire) who have surplus authorizations
Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

RED:
Evaluated Risk - High
If user mapping can be maintained, access as a different user is possible. This is very critical in an SSO environment.

Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02 DICBERCLS=SCUS
Object 3: S_USER_GRP with ACTVT=02

2.1.5.5 SAP User IDs Have More Than One SNC User Attached (0595)

Purpose
Normally SNC names can log on with one user name only. However, for special purposes it may be necessary for some users to log on with other user names as well. This may be the case for special users such as DDIC. As this creates a higher risk in general, all these users have to be displayed so that the customer is aware of the risk.

Procedure
The system checks table USRACL to see whether one SNC name is mapped to more than one user name.

Risk Rating
This check is not rated. It is for information purposes only.
YELLOW:
The table above contains all SNC names that are allowed to log on with more than one SAP user.
Recommendation:
To reduce risk, limit the number of these users.

2.1.6 Single Sign-On (SSO) Ticket

2.1.6.1 Unspecified Accepting of SSO Tickets (0603)

**Purpose**
Customers must be aware of ALL trusted Single Sign On (SSO) connections into their systems.

**Procedure**
Customers have to enter all their connections in the questionnaire. If the system finds additional connections, they are entered in the results table of this check.

**Risk Rating**
The rating is done automatically as follows:
- GREEN: No additional connections
- RED: Additional connections that were not mentioned in the questionnaire

**Evaluated Risk - High**
The system found that you accept SSO tickets from more systems than specified in the questionnaire.

Recommendation:
Check the entries in table TWPSSO2ACL by using transaction SE16 or SM30 or STRUSTSSO2. Table TWPSSO2ACL contains all systems from which you accept SSO tickets.

2.1.6.2 Users - Other Than System Administrators - Are Authorized to Maintain the SSO Configuration (0604)

**Purpose**
Find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):
- **Green**: No users found (except those specified in the questionnaire) who have surplus authorizations
- **Yellow/Red**: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.
- **RED**: Evaluated Risk - High

SSO is in use in this system. It is critical that more users than just the system administrators are allowed to maintain the SSO configuration.

Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization Objects:**
- **Object 1**: S_TCODE with TCD=SM30 or TCD=SM31 or TCD=SE16 or TCD=SE16N [as well as all relevant parameter transactions]
- **Object 2**: S_TABU_DIS with ACTVT=02 DICBERCLS=SS
- **Object 3**: S_RZL_ADM with ACTVT=01
- **Object 4**: S_ADMI_FCD with S_ADMI_FCD=NADM
### 2.1.6.3 Users - Other Than System Administrators - Are Authorized to Maintain Trusted SSO Ticket Issuing Systems (0605)

**Purpose**
Find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):
- **Green:** No users found (except those specified in the questionnaire) who have surplus authorizations
- **Yellow/Red:** Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - High**
Table TPWSS02ACL contains all systems that are trusted issuers of SSO tickets. Therefore, only system administrators must be authorized to maintain this table. Otherwise the problem arises that more systems could be entered from here.

**Recommendation:** Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization Objects:**
- **Object 2:** S_TCODE with TCD=SM30 or TCD=SM31 or TCD=SE16 or TCD=SE16N [as well as all relevant parameter transactions]
- **Object 2:** S_TABU_DIS with ACTVT=02 DICBERCLS=SS
- **Object 3:** S_RZL_ADM with ACTVT=01
- **Object 4:** S_ADMI_FCD with S_ADMI_FCD=NADM

### 2.1.6.4 Validity Period for the SSO Ticket Is Too Long (0607)

**Purpose**
As logon tickets allow access to systems without a new password check, they must be limited to a reasonable timeframe.

**Procedure**
The system checks the profile parameter login/ticket_expiration_time if SSO2 usage is activated (login/create_sso2_ticket).

**Risk Rating**
The rating is done automatically as follows:
- **GREEN:** The expiration time is less than 12 hours.
- **YELLOW:** The expiration time is 12 to 24 hours.
- **RED:** The expiration time is more than 24 hours.

**Evaluated Risk - High**
Think about reducing this parameter to a value of less than 12 hours. This parameter controls the expiration time of the SSO tickets to your SAP system. This must be restricted because the system is open to misuse if the desktop is not sufficiently protected.

**Evaluated Risk - Medium**
Think about reducing this parameter to a value less than 12 hours. This parameter controls the expiration time of the SSO2 tickets to your SAP system. This must be restricted because the system is open to misuse if the desktop is not sufficiently protected.
2.1.6.4.1 Validity Period for the SSO Ticket Is Too Long (0607)

2.1.6.5 SSO Ticket Can Be Sent via an Unsecured Connection (0608)

**Purpose**
Single Sign On (SSO) tickets must be sent by https only. Otherwise, they could be intercepted during data transmission, and anybody could then log on as the user that requested this SSO ticket.

**Procedure**
The system checks the profile parameter login/ticket_only_by_https.

**Risk Rating**
The rating is done automatically as follows:
GREEN: The parameter is set to 1.
RED: The parameter is set to 0.

**Evaluated Risk - High**
Recommendation:
Set the parameter login/ticket_only_by_https to 1 to ensure that the SSO tickets can be transferred only when encrypted. Otherwise, they could be intercepted by somebody else during the transmission.

2.1.6.5.1 SSO Ticket Can Be Sent via an Unsecured Connection (0608)

2.1.7 Certificate SSO

2.1.7.1 External Authentication via Client Certificates (0621)

**Purpose**
To check whether external authentication by means of client certificates is allowed.

**Procedure**
The system checks whether table USREXTID contains at least one entry of type DN (Distinguished Name).
For release 4.6 (certificate logon by means of SAP Internet Transaction Server (ITS)):
The system checks the system profile parameters (snc/extid_login_diag = 1 OR snc/extid_login_rfc = 1) AND snc/enable=1 AND table SNCSYCACL is not empty.
As of SAP Web Application Server 6.10, in addition to the certificate logon by means of ITS, the system also checks the certificate logon by means of Internet Communication Manager (ICM):
The system checks the system profile parameters icm/HTTPS/verify_client >= 1 AND that the function module TH_PLUGINS_ACTIVE returns "https".

**Risk Rating**
The check is performed automatically.
The risk is not rated. The check indicates whether external authentication is enabled.
YELLOW:
External authentication by means of client certificates to log on to your system is enabled. Therefore, the system performs the following checks to try to reduce the vulnerability of the corresponding settings.

2.1.7.2 Trusted Certification Authorities (0623)

**Purpose**
To check the specified Certification Authorities (CAs) for SAP Web Application Server.

**Procedure**
The content of table STRUSTCERT is listed.
Risk Rating
The check is performed automatically. The risk is not rated. The check indicates whether table STRUSTCERT is empty.
You currently trust the following certification authorities (CA):
(This can be changed in transaction STRUST.)

2.1.7.3 Users - Other Than System Administrators - Are Authorized to Maintain Trusted CAs (0624)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

Green: No users found (except those specified in the questionnaire) who have surplus authorizations

Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
If more people are allowed to maintain the trusted certification authorities (CA), the risk arises that fake CAs are trusted as well.
Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=STRUST [as well as all relevant parameter transactions]
Object 2: S_RZL_ADM with ACTVT=01
Object 3: S_ADMI_FCD with S_ADMI_FCD=NADM

2.1.7.4 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSAACL via SNC0 (0625)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

Green: No users found (except those specified in the questionnaire) who have surplus authorizations

Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
Table SNCSYSAACL contains the SNC name of all ITS AGates that are allowed to pass a user certificate to the system for authentication. Everybody who is allowed to maintain this table can create backdoor access by means of an unauthorized ITS AGate to the SAP system.
Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You
can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SNC0 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02, DICBERCLS=SCUS
Object 3: S_TABU_CLI with CLIIDMAINT=X
Object 4: S_ADMI_FCD with S_ADMI_FCD=NADM

2.1.7.5 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via Table Maintenance (0626)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

- **Green**: No users found (except those specified in the questionnaire) who have surplus authorizations
- **Yellow/Red**: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

**RED:** Evaluated Risk - High

Table SNCSYSACL contains the SNC name of all ITS AGates that are allowed to pass a user certificate to the system for authentication. Everybody who is allowed to maintain this table can create backdoor access by means of an unauthorized ITS AGate to the SAP system.

Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02, DICBERCLS=SCUS
Object 3: S_TABU_CLI with CLIIDMAINT=X
Object 4: S_ADMI_FCD with S_ADMI_FCD=NADM

2.1.7.6 Users - Other Than User Administrators - Are Authorized to Maintain the Mapping of X.509 Users to SAP Users (0622)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):

- **Green**: No users found (except those specified in the questionnaire) who have surplus authorizations
- **Yellow/Red**: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.

**RED:** Evaluated Risk - High
SC_AUTHENTICATION - SC Authentication checks

Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02 DICBERCLS=SCUS
Object 3: S_USER_GRP with ACTVT=02

If user mapping can be maintained, access as a different user is possible. This is very critical in an SSO environment.

2.1.8 Pluggable Authentication Services (PAS)

2.1.8.1 External Authentication via the Pluggable Authentication Services Is in Use (0631)

Purpose
If Single Sign-On (SSO) is enabled, you have to check the SSO settings as well. This check is for information purposes only.

Procedure
Check whether the parameter login/accept_sso2_ticket =1 and (up to 4.6C) whether the TWPSSO2ACL table contains at least one entry.

Risk Rating
If SSO is enabled, the check is performed automatically.
No rating.
YELLOW:
SSO is enabled for logging on to your system. The following checks are therefore performed to reduce the vulnerability of the corresponding settings as much as possible.

2.1.8.2 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via SNC0 (0633)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):
Green: No users found (except those specified in the questionnaire) who have surplus authorizations
Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
Table SNCSYSACL contains the SNC name of all ITS AGates that are allowed to pass a user certificate to the system for authentication. Everybody who is allowed to maintain this table can create backdoor access by means of an unauthorized ITS AGate to the SAP system.
Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.
SC_AUTHENTICATION - SC Authentication checks

Authorization Objects:
Object 1: S_TCODE with TCD=SNC0 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02, DICBERCLS=SCUS
Object 3: S_TABU_CLI with CLIIDMAINT=X
Object 4: S_ADMI_FCD with S_ADMI_FCD=NADM

2.1.8.3 Users - Other Than System Administrators - Are Authorized to Maintain Table SNCSYSACL via Table Maintenance (0634)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):
Green: No users found (except those specified in the questionnaire) who have surplus authorizations
Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
Table SNCSYSACL contains the SNC name of all ITS AGates that are allowed to pass a user certificate to the system for authentication. Everybody who is allowed to maintain this table can create backdoor access by means of an unauthorized ITS AGate to the SAP system.
Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE with TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02, DICBERCLS=SCUS
Object 3: S_TABU_CLI with CLIIDMAINT=X
Object 4: S_ADMI_FCD with S_ADMI_FCD=NADM

2.1.8.4 Users - Other Than User Administrators - Are Authorized to Maintain the Mapping of External to SAP Users (0632)

Purpose
Find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (green/yellow/red):
Green: No users found (except those specified in the questionnaire) who have surplus authorizations
Yellow/Red: Multiple users who have surplus authorizations were found. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
Recommendation: Use the Profile Generator (transaction PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) or transaction SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You
can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization Objects:**
Object 1: S_TCODE with TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02 DICBERCLS=SCUS
Object 3: S_USER_GRP with ACTVT=02

If user mapping can be maintained, access as a different user is possible. This is very critical in an SSO environment.
3 SC_BASISADMIN - Security Check Basis Administration

3.1 Basis Administration and Basis Authorizations

3.1.1 Basis Administration

3.1.1.1 Gateway and Message Server Security (SY084)

**Purpose**
To check selected security aspects with respect to the kernel patch level, SAP gateway, and SAP message server. Download data is analyzed and rated automatically (but individually) for each check. If no download data exists, leave both this check and the subchecks unrated.

**Rating**
The rating is determined automatically from the subchecks.

**Procedure**
Proceed with the subchecks.

3.1.1.1.1 Kernel Patch Level (SY086)

**YELLOW:**
To enable certain gateway security functionality, a minimum kernel patch level is required. Your system does not currently meet this requirement.

**Recommendation:** Update the kernel of your system to the newest kernel patch level available. Update to a kernel patch level equal to or higher than the minimum required kernel patch level specified above. For more information, see SAP Note 1298433.

3.1.1.1.2 Gateway Security (SY085)

3.1.1.1.2.1 Gateway Security Properties (SY087)

**YELLOW:**
The parameter GW/REG_NO_CONN_INFO controls the activation of certain security properties of the SAP gateway. It is defined as a bit mask with one bit per property.

SAP Note 1298433 “Bypassing security in reginfo & secinfo” is not activated in your system. The bit mask value for bit 1 is not set.

**Recommendation:** Enable the missing property by adding the bitmask value to the current value of GW/REG_NO_CONN_INFO. For more information about GW/REG_NO_CONN_INFO, see SAP Note 1444282.

3.1.1.1.2.2 Enabling an Initial Security Environment (SY088)

**Recommendation:** Parameter gw/acl_mode can be set to 1 to activate a more secure default behavior if either of the access control lists defined by gw/sec_info and gw/reg_info does not exist.

SAP recommends setting gw/acl_mode to 1 to establish an additional line of defense should any of the access control lists be missing. For more information, see SAP Note 1480644.

3.1.1.1.2.3 Gateway Access Control Lists (SY089)

**Recommendation:** The profile parameters gw/sec_info and gw/reg_info provide the file names of the corresponding access control lists. These access control lists are critical to controlling RFC access to your system, including connections to RFC servers. You should
create and maintain both access control lists, which you can do using transaction SMGW. For more information, see "Configuring Connections between SAP Gateway and External Programs Securely" on SAP Help Portal.

3.1.1.1.3 Message Server Security (SY091)

3.1.1.1.3.1 Separation of Internal and External Message Server Communication (SY092)

Recommendation: Communication with the message server should be separated into SAP system internal communication (TCP/IP port defined by rdisp/msserv_internal) and communication from user SAPGUIs to the system (TCP/IP port defined by rdisp/msserv), for example. Network firewalls should block access to the port specified in rdisp/msserv_internal from outside the SAP system.

Set parameter rdisp/msserv_internal to a TCP/IP port number different to the port number specified in rdisp/msserv and additionally protect access to the internal message server port by appropriate firewalls. For more information, see SAP Note 821875.

3.1.1.1.3.2 Message Server Administration Allowed for External Clients (SY093)

Recommendation: SAP recommends blocking external administration of the message server by setting the value of both of the profile parameters ms/monitor and ms/admin_port to 0. For more information, see SAP Note 821875.

The ms/admin_port profile parameter can be set dynamically by calling transaction SMMS and choosing Goto -> Security Settings.

3.1.1.1.3.3 Message Server Access Control List (SY094)

Recommendation: The profile parameter ms/acl_info provides the file name of the message server’s access control list. This list controls which application servers are allowed to log on to the message server. SAP recommends defining and properly maintaining this list to prevent rogue application servers from accessing the system. For more information, see SAP Note 821875.

3.1.1.2 Users - Other Than System Administrators - Are Authorized to Maintain System Profiles (0152)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

EVALUATED RISK - HIGH
This authorization allows security-critical system profile parameters to be disabled, otherwise the system might not be able to restart due to an incorrect configuration.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.

For this check examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object1: S_TCODE with TCD=RZ10 [as well as all relevant parameter transactions]
Object2: S_RZL_ADM with ACTVT=01
3.1.1.3 Users - Other Than System Administrators - Are Authorized to Start/Stop Application Servers (0154)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**
**Evaluated Risk - High**
The system might be unavailable due to unauthorized starting and stopping of servers.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object1: S_TCODE with TCD=RZ03 [as well as all relevant parameter transactions]
Object2: S_RZL_ADM with ACTVT=01

3.1.1.4 Users - Other Than System Administrators - Are Authorized to Start/Stop Workprocesses (0156)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**
**Evaluated Risk - High**
Unauthorized process administration can result in inconsistencies in processing.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object1: S_TCODE with TCD=SM04 or TCD=SM50 or TCD=SM51 [as well as all relevant parameter transactions]
Object2: S_ADMI_FCD with S_ADMI_FCD = PADM

3.1.1.5 Users - Other Than System Administrators - Are Authorized to Lock/Unlock Transactions (0157)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.
Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:
Evaluated Risk - High
Risk of unavailability of transactions due to incorrect configuration, or access to locked transactions might be possible.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object1: S_TCODE with TCD=SM01 [as well as all relevant parameter transactions]
Object2: S_ADMI_FCD with S_ADMI_FCD = TLCK

3.1.1.6 Users - Other Than System Administrators - Are Authorized to Maintain Other User’s Lock Entries (0159)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:
Evaluated Risk - High
Inconsistencies due to incorrect deletion of locks are possible.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object1: S_TCODE with TCD=SM12 [as well as all relevant parameter transactions]
Object2: S_ENQUE with S_ENQ_ACT = * or S_ENQ_ACT=ALL or S_ENQ_ACT = DLFU

3.1.1.7 Users - Other Than System Administrators - Are Authorized to Maintain Own Lock Entries (0166)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
YELLOW:
Evaluated Risk - Medium
Inconsistencies due to incorrect deletion of locks are possible.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object1: S_TCODE with TCD=SM12 [as well as all relevant parameter transactions]
Object2: S_ENQUE with S_ENQ_ACT = * or S_ENQ_ACT=ALL or S_ENQ_ACT = DLOU

3.1.1.8 Users - Other Than System Administrators - Are Authorized to Delete or Reprocess Broken Updates (0161)
Purpose
To find users who have more authorizations than they need for their tasks.
Procedure
ST14 download data is analyzed and rated automatically.
Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:
Evaluated Risk - High
Inconsistencies due to incorrect deletion or reprocessing of updates are possible.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object1: S_TCODE with TCD=SM13 [as well as all relevant parameter transactions]
Object2: S_ADMI_FCD with S_ADMI_FCD = UADM

3.1.1.9 Users - Other Than System Administrators - Are Authorized to Activate a Trace (0163)
Purpose
To find users who have more authorizations than they need for their tasks.
Procedure
ST14 download data is analyzed and rated automatically.
Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:
Evaluated Risk - High
Low system performance due to activated SQL trace (ST01).
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD = ST01 or ST05 [as well as all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD = ST0M
3.1.1.10 System Profiles Are Not Consistent (0153)

**Purpose**
The profiles are stored in the database. They are then activated in the file system and are used from there. Transaction RZ10 is used for this process. We strongly recommend that you keep both versions synchronized.

**Procedure**
The system runs a report similar to the following menu item:
RZ10->Profile->Comparisons->Profile in Database-> with active profile.

**Risk Rating**
The rating is done automatically as follows:
GREEN: The profiles are consistent.
RED: The profiles in the database are not consistent with the profile in the file system.

**Evaluated Risk - High**
The profiles in your system are not synchronized. At least one profile has differences between the database and the file system version.

Recommendation:
Import the profile from all active servers to get the latest state that is currently used into the database. As of now, ONLY update by using transaction RZ10, and try to activate all changes in the file system soon afterwards.

3.1.1.11 Table TPFID Contains OS Passwords (0155)

**Purpose**
To check if the the table TPFID contains valid passwords of operating system users.

**Procedure**
The system checks the field PASSWD in the table TPFID.

**Risk Rating**
The rating is done automatically as follows:
GREEN: Table TPFID does not contain any password values.
RED: Table TPFID contains valid logon data or password can be guessed due to maintained data.

**Evaluated Risk - High**
The table TPFID still contains passwords of SAP operating system users. This is from older releases where these passwords were used for starting and stopping remote application servers.

Recommendation:
As these passwords are not encrypted and not used any more, we recommend that you remove them from this table.

3.1.1.12 No Critical Transactions Are Locked (0158)

**Purpose**
Every SAP system has many transactions that are not used in a specific customer environment. As some of these can cause problems if they are used "incorrectly", we recommend that you lock these transactions.

**Procedure**
The system checks the TSTC table in the CINFO field on the hex value X20.

**Risk Rating**
The rating is done automatically as follows:
GREEN: At least two transactions are locked.
RED: Less than two transactions are locked.
YELLOW:
Every SAP system has many transactions that are not used in a specific customer environment.
environment. As some of these can cause problems if they are used "incorrectly", we recommend that you lock these transactions. Currently, either none or a maximum of one transaction has been locked by means of transaction SM01.

Recommendation:
Find out which additional transactions must be locked in your specific environment. You can maintain these transactions by using transaction SM01.

3.1.1.13 No Timely Accurate Resolution of Erroneous Locks (0160)

**Purpose**
SAP enqueue locks may stay in the database after users terminate their sessions. This may result in inconsistencies and other lock issues if nobody maintains old locks and perhaps removes them if an error occurs.

**Procedure**
The system checks for locks that are older than 2 days for each client.

**Risk Rating**
The rating is done automatically as follows:
GREEN: No locks are older than 2 days.
YELLOW: At least 1 lock is older than 2 days.
RED: At least 20 locks are older than 2 days.

**Evaluated Risk - Medium**
Locks may stay in the database after users terminate their sessions incorrectly. This may result in inconsistencies and other lock issues if nobody maintains old locks and perhaps removes them if an error occurs.

Recommendation:
Always look for old locks in your system. You can do this by using transaction SM12. If you find locks that are older than 1 day or from yesterday, ask the users what might have caused these locks so that you can prevent them in future. Finally, if you discover that the locks no longer need to be in the system, delete them.

3.1.1.14 No Timely Accurate Resolution of Broken Updates (0162)

**Purpose**
Terminated updates happen when configuration errors or other problems occur in the system. This may result in inconsistencies later because these updates are not performed in the database. It is therefore essential that you check them and handle the terminated ones carefully.

**Procedure**
The system checks for terminated updates older than 2 days for each client.

**Risk Rating**
The rating is done automatically as follows:
GREEN: No terminated updates are older than 2 days.
YELLOW: At least 1 terminated update is older than 2 days.
RED: At least 20 terminated updates are older than 2 days.

**Evaluated Risk - Medium**
Always look for old terminated updates in your system. You can do this by using transaction SM13. If you find terminated updates, ask the users what might have caused them so that you can prevent them in the future.

Recommendation:
As these updates have not been written to the database by now, but the application would normally expect this, you have to discuss how to proceed with the person responsible for this application. If you delete the updates, this may make the SAP database inconsistent.
3.1.1.15 Security Audit Log is not active (0170)

**Purpose**
The Security Audit Log records security-related events, such as unsuccessful logon attempts or unsuccessful transaction starts. This log is a tool designed for auditors who need to take a detailed look at what occurs in the SAP system.

**Procedure**
The system checks the profile parameters rsau/enable.

**Risk Rating**
Rating takes place automatically as follows:
- GREEN: Profile parameters rsau/enable = 1.
- RED: Profile parameters rsau/enable = 0.

**Evaluated Risk - High**
The Security Audit Log provides for long-term data access. The audit files are retained until you explicitly delete them.

Among others, you can record the following information:
- Successful and unsuccessful dialog logon attempts
- Successful and unsuccessful RFC logon attempts
- RFC calls to function modules
- Changes to user master records
- Successful and unsuccessful transaction starts
- Changes to the audit configuration

Other checks within the SOS related to the Security Audit Log:
- Normal Users Are Not Logged in the Security Audit Log (0136)
- User SAP*'s activities are not logged in the SAL (0047)
- User DDIC's activities are not logged in the SAL (0050)
- User SAPCPIC's activities are not logged in the SAL (0055)
- User EARLYWATCH's activities are not logged in the SAL (0060)
- Logging of OSS User Activities in the SAL? (0533)

**Recommendation to customize the Security Audit Log.**

- Activate the profile parameter rsau/enable.
- Set the profile parameter rsau/selection_slots to its maximum value of 10.
- Activate the profile parameter rsau/user_selection.

**Filter:**
- Use one filter to log critical events for all users in all clients.
- Use other filters to log everything for critical users such as SAP* and support users, including FireFighter users.
- Use the remaining filters to log events in special cases.

3.1.1.16 System Recommendations (ABAP) (SY123)

**Purpose**
To check whether the System Recommendations tool is being used. This is a mandatory prerequisite for setting up a strong security patch process.

For further recommendations, refer to [http://support.sap.com/sysrec](http://support.sap.com/sysrec).

**Procedure**
This check is analyzed and rated automatically. No further action is necessary.

**Rating**
The rating is set automatically.
- GREEN: The System Recommendations tool is used and shows results that are up to 31
days old.

**YELLOW:**
- The System Recommendations tool is used but the results are older than 31 days.
- The System Recommendations tool is not used for this system.
- The System Recommendations tool is not used at all.

**RED:**
*Comment Line: DO NOT DELETE OR CHANGE!*
*Comment Line: Text is being created during runtime.*

**YELLOW:**
*Comment Line: DO NOT DELETE OR CHANGE!*
*Comment Line: Text is being created during runtime.*

**GREEN:**
*Comment Line: DO NOT DELETE OR CHANGE!*
*Comment Line: Text is being created during runtime.*

**Recommendation:** SAP strongly recommends applying important security fixes as soon as possible.

The 'System Recommendations' application provides a detailed recommendation regarding which SAP security notes (ABAP and non-ABAP) should be implemented based on the actual status of the system and the notes already implemented. This is a mandatory prerequisite for setting up a strong security patch process. For more information, refer to [http://support.sap.com/sysrec](http://support.sap.com/sysrec).

### 3.1.1.17 Sending Trace Data to Remote Client (0169)

**Purpose**
To checks if it is allowed that the system provides trace data to a remote client.

**Procedure**
The system checks the profile parameter rdisp/accept_remote_trace_level.

**Risk Rating**
The rating is done automatically as follows:
GREEN: The parameter is set to 0 (Remote trace disabled).
YELLOW: The parameter is set to 1 (Remote trace enabled).

**YELLOW:**
*Evaluated Risk - Medium*
The parameter rdisp/accept_remote_trace_level allows that the system provides trace data to a remote client.

Recommendation:
Deactivate the profile parameter if you do not need trace data at a remote client.

#### 3.1.1.17.1 Sending Trace Data to Remote Client (0169)

### 3.1.2 Batch Input

#### 3.1.2.1 No Timely Accurate Resolution of Failed Batch Input Sessions (0223)

**Purpose**
Batch input is a frequently used technique for importing data into the SAP system. This is done on a regular basis. As productive data is imported into the SAP system, it is necessary to check all failed batch input sessions so that no data is lost.

**Procedure**
The system checks for batch input sessions that are older than 2 days.

**Risk Rating**
The rating is done automatically as follows:
GREEN: Up to 4 failed sessions.
YELLOW: 5 or more failed sessions.
**Evaluated Risk - Medium**
Batch input is a frequently used technique for importing data into the SAP system. This is done on a regular basis. As productive data is imported into the SAP system, it is necessary to check all failed batch input sessions so that no data is lost.

Recommendation:
Always check whether failed batch input sessions exist by using transaction SM35 on a regular basis and correct them.

**3.1.2.2 Users - Other Than Batch Input Administrators - Are Authorized to Run Batch Input Sessions in Dialog (0221)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**Evaluated Risk - Medium**
This authorization allows batch input data to be manipulated during online processing.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SM35 [as well as all relevant parameter transactions]
Object 2: S_BDC_MONI with BDCAKTI=AONL

**3.1.2.3 Users - Other Than Batch Input Administrators - Are Authorized to Administer Batch Input Sessions (0222)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**Evaluated Risk - Medium**
This authorization allows batch input maps to be deleted or locked with the risk of system inconsistency.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SM35 [as well as all relevant parameter transactions]
Object 2: S_BDC_MONI with BDCAKTI=DELE or BDCAKTI=LOCK
3.1.3 Spool & Printer

3.1.3.1 Users - Other Than Spool Administrators - Are Authorized to Display Other Users Spool Requests (0192)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**Evaluated Risk - High**
This authorization allows unauthorized access to sensitive data contained in spool requests.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
1. S_TCODE with TCD = SP01 or SP01O [as well as all relevant parameter transactions]
2. S_ADMI_FCD with S_ADMI_FCD = SP01 or SP0R
3. S_SPO_ACT with SPOACTION = BASE and DISP and SPOAUTH = * or ___USER___

3.1.3.2 Users - Other Than Spool Administrators - Are Authorized to Display Protected Spool Requests of Other Users (0198)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**Evaluated Risk - High**
This authorization allows unauthorized access to sensitive data contained in protected spool requests.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
1. S_TCODE with TCD = SP01 or SP01O [as well as all relevant parameter transactions]
2. S_ADMI_FCD with S_ADMI_FCD = SP01 or SP0R
3. S_SPO_ACT with SPOACTION = BASE and DISP and SPOAUTH = * or ___USER___
3.1.3.3 Users - Other Than Spool Administrators - Are Authorized to Display the TemSe Content (0193)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:

**Evaluated Risk - High**
This authorization allows unauthorized access to sensitive data contained in spool requests.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD = SP11 or TCD = SP12 [as well as all relevant parameter transactions]
Object 2: S_TMS_ACT with STMSACTION = REA and (STMSOWNER = GRP or OCL) and STMSOBJECT = SPOOL*

3.1.3.4 Users - Other Than Spool Administrators - Are Authorized to Change the Owner of Spool Requests (0194)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:

**Evaluated Risk - High**
This authorization allows unauthorized access to sensitive data contained in spool requests after the ownership has been changed.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD = SP01 [as well as all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD = SP01 or SP0R
Object 3: S_SPO_ACT with SPOACTION = USER

3.1.3.5 Users - Other Than Spool Administrators - Are Authorized to Redirect a Print Request to Another Printer (0195)

**Purpose**
To find users who have more authorizations than they need for their tasks.
**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
This authorization allows unauthorized access to sensitive data after a request has been redirected.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD = SP01 [as well as all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD = SP01 or SP0R
Object 3: S_SPO_ACT with SPOACTION = REDI

---

**3.1.3.6 Users - Other Than Spool Administrators - Are Authorized to Export a Print Request (0196)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
This authorization allows unauthorized access to sensitive data after the spool request has been exported.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD = SP01 [as well as all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD = SP01 or SP0R
Object 3: S_SPO_ACT with SPOACTION = DOWN

---

**3.1.3.7 Users - Other Than Spool Administrators - Are Authorized to Print on all Devices (0197)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

YELLOW:

Evaluated result:
More than 20% of your users, of at least one client, can print on all devices.
When sensitive data is output, it can be sent to the wrong printer accidentally and could be
accessed by an unauthorized employee.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain
Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending
on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization object:
Object1: S_SPO_DEV with SPODEVICE = *.

3.1.4 Background

3.1.4.1 Periodic Background Jobs Scheduled with User of Type Other Than
'SYSTEM' (0211)

Purpose
Periodic background jobs should be scheduled under a user ID of an anonymous user. User
IDs of natural persons must not be used, because if you delete this user, background
processing would be affected.

Procedure
The system checks the users of the periodic background jobs.

Risk Rating
The rating is done automatically as follows.
GREEN: All periodic background jobs are scheduled under a user ID of an anonymous user.
YELLOW: Up to 20% of the periodic background jobs are scheduled under a user ID of a
natural person.
RED: More than 20% of the periodic background jobs are scheduled under a user ID of a
natural person.

RED:
Evaluated Risk - High
Periodic background jobs must be scheduled under an anonymous user ID, for example
Batchuser, and not under the ID of an individual. If an ID of an individual is used for
background jobs and at some point the user is deleted or locked, background processing
would be affected. Therefore, an anonymous user ID is necessary.

In your system, more than 20% of the periodic background jobs are scheduled under a non-
anonymous user ID.

YELLOW:
Evaluated Risk - Medium
Periodic background jobs must be scheduled under an anonymous user ID, for example
Batchuser, and not under the ID of an individual. If an ID of an individual is used for
background jobs and at some point the user is deleted or locked, background processing
would be affected. Therefore, an anonymous user ID is necessary.

In your system, more than 20% of the periodic background jobs are scheduled under a non-
anonymous user ID.

3.1.4.2 Background Users That Are Not Used in Any Periodic Batch Job (0215)

Purpose
To avoid misuse of unused background users (who probably have too many authorizations)
**Procedure**
The system checks which users of user type 'B' are not used in periodic jobs.

**Risk Rating**
The rating is done automatically as follows.
GREEN: No unused background user was found.
YELLOW: At least one unused background user was found.

**YELLOW:**
There is at least one unused user of user type 'system' ('B') in your system.
Unused batch users who probably have many authorizations can be misused. These users do not occur in your periodic jobs and therefore seem to be unused.

### 3.1.4.3 Users - Other Than Background Administrators - Are Authorized to Schedule Jobs in SM36 (0212)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
Unauthorized background administration can result in:
- Inconsistencies
- Loss of information
- Unauthorized execution of critical programs

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.

For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
1. **Object 1:** S_TCODE with TCD=SM36 [as well as all relevant parameter transactions]
2. **Object 2:** S_BTCH_ADM with BTCADMIN=Y  OR  
3. **Object 3:** S_BTCH_JOB with JOBACTION = RELE

### 3.1.4.4 Users - Other Than Background Administrators - Are Authorized to Schedule Jobs in External Commands (0213)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
This authorization allows unauthorized execution of external programs or commands.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending
on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below. 

Authorization objects:
Object 1: S_TCODE with TCD=SM36 [as well as all relevant parameter transactions]
Object 2: S_BTCH_ADM with BTCADMIN=Y or S_BTCH_JOB with JOBACT = RELE
Object 3: S_RZL_ADM with ACTVT=01

3.1.4.5 Users - Other Than Background Administrators - Are Authorized to Schedule Jobs Under Another User Id (0214)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

Evaluated Risk - High
This authorization allows you to execute critical reports using another user. The security issue is that this user has more authorization than your own user has. This means using this user you may be able to run critical reports that you otherwise would not be authorized to do.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below. 

Authorization objects:
Object 1: S_TCODE with TCD=SM36 [as well as all relevant parameter transactions]
Object 2: S_BTCH_NAM with BTCUNAME <> '
Object 3: S_BTCH_ADM with BTCADMIN=Y or S_BTCH_JOB with JOBACT = RELE

3.1.5 OS Access

3.1.5.1 Users - Other Than System Administrators - Are Authorized to Define External OS Commands (0171)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

Evaluated Risk - High
Unauthorized maintenance of operating system commands can cause malicious commands to be executed.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending
on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below. Authorization objects:
Object1: S_TCODE with TCD=SM69 [as well as all relevant parameter transactions]
Object2: S_RZL_ADM with ACTVT=01

3.1.5.2 Users - Other Than System Administrators - Are Authorized to Execute External OS Commands (0172)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations. YELLOW:

Evaluated Risk - Medium
Unauthorized execution of dangerous operating system commands mostly as administrator on the application server.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below. Authorization objects:
Object1: S_TCODE with TCD=SM49 [as well as all relevant parameter transactions]
Object2: S_LOG_COM

3.1.5.3 Users - Other Than System Administrators - Are Authorized to View Content of OS Files with AL11 (0173)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations. RED:

Evaluated Risk - High
Unauthorized access to sensitive data stored in files at operating system level, for example /etc/passwd on UNIX and interface files with sensitive data.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below. Authorization objects:
Object 1: S_TCODE with TCD=AL11 [as well as all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD = ST0R
Object 3: S_DATASET with PROGRAM = RSWATCH0 ACTVT = 33
3.1.6 Outgoing RFC

3.1.6.1 Unsecured Outgoing RFC Calls (0252)

**Purpose**
To check the authenticity of the calling system.

**Procedure**
The system checks:
- whether the profile parameter is snc/enable=1
- whether table RFCDESSECU contains the name of the RFC destination to be secured by means of SNC.

**Risk Rating**
The rating is done automatically as follows:
GREEN: SNC is enabled and RFC destinations are SNC-protected.
YELLOW: Either SNC is disabled or non-SNC-protected RFC connections exist.

**Evaluated Risk - Medium**
Secure Network Communication (SNC) is disabled for your system, or a non SNC protected RFC connections exist.

3.1.6.2 SNC Protection for encrypted outgoing RFC calls (0253)

**Purpose**
To avoid eavesdropping due to unencrypted communication data.

**Procedure**
The system checks for all RFC destinations with active SNC settings if SNC is active in general (profile parameter snc/enable = 1), and if the SNC options for those RFC destinations provide encryption. This is the case for following settings concerning the Quality of Protection (QOP):
- QOP = '3' OR
- QOP = '8' AND profile parameter snc/data_protection/use = 3 OR
- QOP = '9' AND profile parameter snc/data_protection/max = 3

**Risk Rating**
Rating takes place automatically as follows:
GREEN: Case 1: No RFC destination is enabled for SNC.
Case 2: At least one SNC-protected RFC destination exists and all SNC-protected RFC destinations provide encryption and SNC is enabled.
RED: At least one SNC-protected RFC destination exists. In addition, some of these RFC destinations do not provide encryption or SNC is not enabled.

**Evaluated Risk - High**
At least one SNC-protected RFC destination exists. In addition, some of these RFC destinations do not provide encryption or SNC is not enabled (profile parameter snc/enable = 0).

3.1.6.3 Unexpected RFC Connections with Complete Logon Data Found (0254)

**Purpose**
To prevent the misuse of RFC connections to access other systems.

**Procedure**
The system checks table RFCDES and searches for entries where the field RFCOPTIONS contains the string 'V=<encrypted password>'.

**Risk Rating**
Rating takes place automatically as follows:
GREEN: No additional RFC connection with complete logon data.
RED: At least one additional RFC connection with complete logon data.
RED:
**Evaluated Risk - High.**
There is at least one additional RFC connection with complete logon data. The following RFC destinations contain complete logon data. As these connections were not mentioned in the questionnaire, we assume that they were not known to you. In special cases, a direct logon to the target system without any further password check could be possible. Check these destinations in greater detail.

**Recommendation**
Use report RSRFCCHK to analyze RFC destinations with complete logon information. Ensure that the remote users have the correct user type (usually the user type "system" and not "dialog") and have only restricted authorizations, as required. Consider using the "Authorization for Destination", which you can set on the "Logon&Security" tab in transaction SM59, to restrict the use of critical RFC destinations. See SAP Note [1595582](#) "Deletion of temporary RFC destinations" to delete generated RFC destinations with a 32-character GUID as RFC name.

**3.1.6.4 Users - Other Than System Administrators - Are Authorized to Administer RFC Connections (0255)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**
**Evaluated Risk - High**
Unauthorized access to other systems.
Malfunction of interfaces if invalid connection data is entered.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below. *Command Line: IF "YSAP-R3_REL" <= '7.00'.*

**Authorization objects:**
Object 1: S_TCODE with TCD=SM59
Object 2: S_ADMI_FCD with S_ADMI_FCD = NADM

*Command Line: ELSE.*

*Command Line: IF "YSAP-NOTE_2226263?" = 'X'.*

**Authorization objects:**
Object 1: S_TCODE with TCD=SM59
Object 2: S_ADMI_FCD with S_ADMI_FCD = NADM
Object 3: S_RFC_ADM with ACTVT NE 03, 39

*Command Line: ELSE.*

*Command Line: ENDIF.*

**Authorization objects:**
Object 1: S_TCODE with TCD=SM59
Object 2: S_ADMI_FCD with S_ADMI_FCD = NADM
Object 3: S_RFC_ADM with ACTVT NE 03

*Command Line: ENDIF.*
3.1.6.5 Users - Other Than System Administrators - Are Authorized to Access RFC Logon Information (0256)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**
**Evaluated Risk - High**
The authorization to view the data in table RFCDES makes it possible for a dictionary attack to find out the password of a user specified in an RFC connection.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SE16 or TCD=SE16N or TCD=SE17 or TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=03 DICBERCLS=SC

3.1.6.6 Unexpected Trusting System Connections Found (0267)

**Purpose**
To prevent unauthorized access by using trusted systems.

**Procedure**
The system checks in table RFCDES whether:
- the selection is RFCTYPE=3
- RFCOPTIONS contains the string Q=Y.

**Risk Rating**
The rating is done automatically as follows:
GREEN: No additional outbound trusted systems.
RED: Additional outbound trusted systems.

**RED:**
**Evaluated Risk - High.**
You have defined more trusting systems than specified in the questionnaire.
Trusted systems are target systems that are configured in the source system for outbound trusted RFC.

3.1.6.7 Users - Other Than System Administrators - Are Authorized to Maintain Trusting Systems (0268)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**
Evaluated Risk - High
This authorization allows users to maintain the trusting systems for outbound trusted RFC communication. A trusted system can afterwards be used for trusted RFC.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SMT2 [as well as all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD = NADM

3.1.6.8 Start of External Server Programs Is Not Restricted (0282)
Purpose
To protect the start of external server programs.

Procedure
The system checks whether the file that is specified in profile parameter gw/sec_info exists (default = secinfo).

Risk Rating
The rating is done automatically as follows:
GREEN: The file secinfo exists for all application servers and is consistent.
RED: The file secinfo does not exist (output in SMGW: External security is deactivated).

Evaluated Risk - High
The secinfo file defined in the profile parameter gw/sec_info does not exist in your system. Therefore, no restrictions apply when external programs are started.
See also SAP Note 614971.

3.1.6.9 Remote Monitoring Function for the RFC Gateway Is Not Disabled (0269)
Purpose
Enabling the monitor functions remotely means that every communication partner can control the gateway. This is not recommended.

Procedure
The system checks the profile parameter gw/monitor.

Risk Rating
The rating is done automatically as follows:
GREEN: The parameter is set to 0 or 1.
YELLOW: The parameter is set to 2.

Evaluated Risk - Medium
Since remote monitoring of the gateway is not necessary, we recommend that you change the parameter gw/monitor to '1' in the default profile.

3.1.6.9.1 Parameter gw/monitor on <;GENERAL; Name>

3.1.6.10 Permit-all simulation mode is active for the RFC gateway (0273)
Purpose
Note 1689663 "GW: Simulation mode for reg_info and sec_info" describes how to enable a permit-all simulation mode for the RFC gateway, which ignores any existing access control entries. Even if this setting makes implementing an access control list for the RFC gateway much easier, it is a security risk to maintain this setting for a long time. We strongly recommend deactivating simulation mode as soon as access control lists should be active.

Procedure
The system checks the profile parameter gw/sim_mode.
Risk Rating
Rating takes place automatically as follows:
GREEN: The value is ‘0’.
RED: The value is ‘1’. This means that even if an access control list is available, any access request is granted to the RFC gateway.

Evaluated Risk - High
Note 1689663 "GW: Simulation mode for reg_info and sec_info" describes how to enable a permit-all simulation mode for the RFC gateway, which ignores any existing access control entries. Even if this setting makes implementing an access control list for the RFC gateway much easier, it is a security risk to maintain this setting for a long time. We strongly recommend deactivating simulation mode as soon as access control lists should be active.

Recommendation:
Set the profile parameter gw/sim_mode to ‘0’ to deactivate simulation mode and to activate access control.

3.1.6.10.1 Parameter gw/sim_mode <;GENERAL; Name>

3.1.7 Incoming RFC

3.1.7.1 Users Are Authorized to Run Any RFC Function (0241)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

Evaluated Risk - High
An unauthorized remote execution of RFC functions with dialog users was detected. All of the following users are authorized to access all SAP RFC-enabled function modules. This is very critical because there are very many RFC-enabled function modules that can be called. In Release 4.6C, for example, there are approximately 14000 RFC-enabled function modules. Not all of them contain special authorization checks. All of the following users can use some of these function modules without additional authorizations.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object: S_RFC with RFC_NAME = *

3.1.7.2 Users - other than Key Users - are Authorized to Visualize All Tables via RFC (0245)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

Evaluated Risk - High
An unauthorized remote execution of RFC functions with dialog users was detected. All of the following users are authorized to access all SAP RFC-enabled function modules. This is very critical because there are very many RFC-enabled function modules that can be called. In Release 4.6C, for example, there are approximately 14000 RFC-enabled function modules. Not all of them contain special authorization checks. All of the following users can use some of these function modules without additional authorizations.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object: S_RFC with RFC_NAME = *
**Evaluated Risk - High**
Unauthorized access to sensitive data by means of RFC. The following users are authorized to access RFC function modules, which allows them to retrieve all SAP tables. As this is a very critical authorization, assign it only as required.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.

For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
1. Object 1: S_RFC with RFC_NAME=SDTX
2. Object 2: S_TABU_DIS with ACTVT=03 AND DICBERCLS=* 

**3.1.7.3 Incoming RFC with Expired Password is Allowed (0234)**

**Purpose**
To prevent undetected use of a user ID with an expired password.

**Procedure**
The system checks the profile parameter rfc/reject_expired_passwd.

**Risk Rating**
The rating is done automatically as follows:
GREEN: The parameter is set to 1.
YELLOW: The parameter is set to 0.

**Evaluated Risk - Medium**

**Recommendation:**
Set the parameter rfc/reject_expired_passwd to 1 to detect the use of a user ID with an expired password.

**IMPORTANT:** Before you change this parameter, import SAP Note [622464](#).

**3.1.7.3.1 Incoming RFC with expired password is allowed (0234)**

**3.1.7.4 Users authorized for Trusted RFC (Object S_RFCACL) (0239)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**Evaluated Risk - Medium**

Unauthorized use of trusted RFC connections. All of the following users are allowed to access the analyzed system using a trusted system connection. We do not rate this check.

**Check whether the users really need this authorization.**

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.

For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects: 
Object: S_RFCACL
Please try to specify the values for the "RFC_SYSID" and "RFC_CLIENT" fields for this authorization object to prevent backdoor entries.

3.1.7.5 Users authorized for Trusted RFC which can be called from any calling user (0248)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.
RED:
Evaluated Risk - High
Unauthorized use of trusted RFC connections. All of the following users can be called using a trusted system connection from any calling user.
Check whether the users really require this authorization.
Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.
For this check examine the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object: S_RFCACL
Use specific values for the "RFC_USER" field instead of using a * value and consider using the 'same user' option instead (field RFC_EQUSER=Y). In this case, you can either leave the "RFC_USER" field empty or you can enter a value that is never used as a user ID (such as the character ").

3.1.7.6 Unexpected Trusted System Connections Found (0238)

Purpose
To prevent unauthorized access by using trusted systems.

Procedure
The system checks the entries in the RFCSYSACL table.

Risk Rating
The rating is done automatically as follows:
GREEN: There are no additional inbound trusted systems.
RED: Additional inbound trusted systems exist.

RED:
Evaluated Risk - High.
You have defined more trusted systems than you specified in the questionnaire.

3.1.7.7 Users - Other Than System Administrators - Are Authorized to Maintain Trusted Systems (0240)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically.

Risk Rating
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
This authorization allows users to maintain trusted systems. A trusted system can subsequently be used for trusted RFC.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.

For this check examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
- Object 1: S_TCODE with TCD=SMT1 [as well as all relevant parameter transactions]
- Object 2: S_ADMI_FCD with S_ADMI_FCD = NADM

### 3.1.7.8 RFC Security in the Service Marketplace (0247)

**Purpose**
To link to an RFC document on the Service Marketplace.

**Procedure**
The document explains how to set up an authorization concept to secure the RFC connections in an SAP system landscape.

**Risk Rating**
No rating for this check. We provide a link to the RFC document on the Service Marketplace.

**YELLOW:**
RFC is a very critical issue for the security of an SAP installation. The following document explains how to set up an authorization concept to secure the RFC connections in an SAP system landscape.

http://service.sap.com/~sapidb/011000358700004954232004E.

### 3.1.8 Protection of Passwords in Database Connections (AB088)

**YELLOW:**
Database user passwords of connected systems can be found in table DBCON. At least one critical record was found in table DBCON. This indicates that at least the manual postprocessing step of SAP Note 1823566 was not performed.

**Recommendation:**
Apply SAP Security Note 1823566 and make sure that you execute the valid manual postprocessing step if you apply the Note correction or the corresponding support package.

**Note:**
This Note is valid for all ABAP installations that use database connections, including when the text focuses on SAP Solution Manager. The Note refers to SAP Solution Manager because typically, many DB connections are maintained.

If this recommendation is displayed, there are DB connections with passwords on the analyzed system. Although transaction DBCO (which you use to maintain such DB connections) does not show the passwords, you can find the obfuscated passwords using transaction SE16 for table DBCON with the field value PASSWORD <> space.

### 3.1.9 Application Link Enabling (ALE)

#### 3.1.9.1 Users - Other Than System Administrators - Allowed to Maintain the ALE Distribution Model (0723)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
Malfunction of ALE communication due to unauthorized changes.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=BD64 [as well as all relevant parameter transactions]
Object 2: B_ALE_MODL with ACTVT = 01 or 02 and CUSTMODEL = *

### 3.1.9.2 Users - Other Than System Administrators - Allowed to Maintain the Partner Profile (0724)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**RED:**

**Evaluated Risk - High**
Malfunction of Application Link Enabling (ALE) communication due to unauthorized changes.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=WE20 [as well as all relevant parameter transactions]
Object 2: S_IDOCPART with ACTVT=01 or ACTVT=02 and EDI_TCD=WE20

### 3.1.9.3 Do You Have any Additional Users with an Authorization to Receive IDOCs (0729)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically.

**Risk Rating**
The rating is done automatically.
GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.
YELLOW or RED: Multiple users found with surplus authorizations.

**YELLOW:**

**Evaluated Risk - Medium**
An unauthorized remote execution of RFC functions with dialog users was detected. All of the following users are authorized to access all SAP RFC-enabled function modules. This is very critical because there are very many RFC-enabled function modules that can be called. In Release 4.6C, for example, there are approximately 14000 RFC-enabled function modules.
Not all of them contain special authorization checks. All of the following users can use some of these function modules without additional authorizations.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results.

For this check examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object: S_RFC with RFC_NAME = *
4 SC_CHANGEMGMT - SC Change Management

4.1 Change Management

4.1.1 Data & Program Access

4.1.1.1 Users - Other Than Key Users - Are Authorized to Start All Reports (0512)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
Check which users have authorization to start all reports by using transactions SA38 and SE38, for example.

Risk Rating
The rating is set automatically.
GREEN: Only key users can use SA38, SE38, and so on.
RED: Additional users have authorization to start reports by using SA38, SE38, and so on.

Evaluated Risk - High
GREEN:
Evaluated Risk - None

Execution of critical function reports that do not contain any authorization checks.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE38 or TCD=SA38 or TCD=SC38 [as well as all relevant parameter transactions]
Object 2: S_PROGRAM with P_ACTION=SUBMIT P_GROUP=* 
Remark: We also search for the transaction codes used in parameter transactions defined in table TSTCP. (This is done in every check in which object S_TCODE is checked.) Any user who is authorized to call a transaction defined in table TSTCP that is based on transaction SA38 appears in this check if they also have authorization for the other objects checked.

4.1.1.2 Users - Other Than Key Users - Are Authorized to Display All Tables (0513)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED:
Evaluated Risk - High
GREEN:

**Evaluated Risk - None**

Unauthorized access to sensitive data.

**Recommendation:**

Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

**Authorization objects:**

Object 1: S_TCODE with TCD=SE16 or TCD=SE16N or TCD=SE17 or TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]

Object 2: S_TABU_DIS with ACTVT=03 DICBERCLS=* 

### 4.1.1.3 Users Are Authorized to Maintain All Tables (0514)

**Purpose**

To find users who have more authorizations than they need to perform their tasks.

**Procedure**

ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**

The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).

**YELLOW/RED:** Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

Unauthorized maintenance of sensitive data.

**Recommendation:**

Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

**Authorization objects:**

Object 1: S_TCODE with TCD=SE16 or TCD=SE16N or TCD=SE17 or TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]

Object 2: S_TABU_DIS with ACTVT=02 DICBERCLS=* 

### 4.1.1.4 Users - Other Than System Administrators - Are Authorized to Change the Authorization Group of Tables (0515)

**Purpose**

To find users who have more authorizations than they need to perform their tasks.

**Procedure**

ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**

The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).

**YELLOW/RED:** Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
Unauthorized access to data after change of authorization group.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SE17 or TCD=SM30 or TCD=SM31 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02 DICBERCLS=SS

4.1.1.5 Users - Other Than Query Administrators - Are Authorized to Administer Queries (0517)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED: Evaluated Risk - High
GREEN:

4.1.1.6 Users Are Authorized to Execute All Function Modules (0520)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED: Evaluated Risk - High
GREEN:
Evaluated Risk - None
Execution of critical function modules that do not contain any authorization checks.
Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Command Line: IF "YSAP-R3_REL" <= '6.30'.
Authorization objects:
Object 1: S_TCODE with TCD = SE37 [as well as all relevant parameter transactions]
Object 2: S_DEVELOP with ACTVT = 03 and S_DEVELOP with OBJTYPE = FUGR
Command Line: ELSE.
Authorization objects:
Object 1: S_TCODE with TCD = SE37 [as well as all relevant parameter transactions]
Object 2: S_DEVELOP with ACTVT = 16 and S_DEVELOP with OBJTYPE = FUGR
Command Line: ENDIF.

4.1.2 Change Control

4.1.2.1 System Change Option Not Appropriately Configured in the Production System (0301)

Purpose
To check whether the System Change option is set to 'Not modifiable' (changes to programs are not permitted).

Procedure
Check table TADIR for PGMID=HEAD and OBJ=SYST and whether EDTFLAG = N or P. This can be checked manually with transaction SE06.

Risk Rating
The rating is set automatically as follows:
GREEN: System Change option is set to 'Not modifiable'.
RED: System Change option is set to 'Modifiable'.

Evaluated Risk - High
Threats that arise with the possibility of development in production systems:
- Malfunction of system due to programs that have not been tested properly
- Unauthorized data access with modified or self-developed programs

Recommendation:
Set the System Change Option to 'Not modifiable' in SE06.

4.1.2.2 Client Change Option Not Appropriately Configured (0302)

Purpose
To check whether the Client Change option is set to 'Not modifiable' (changes to programs are not permitted).

Procedure
Check table T000 for all clients, whether CCCORACTIV=2 and CCNOCLIIND=3. CCCATEGORY=P means production client.

Risk Rating
The rating is set automatically as follows:
GREEN: Setting in all clients:
- Changes and transports for client-specific objects set to 'No changes allowed'.
- Cross-client object changes set to 'No changes to Repository and cross-client Customizing obj'.
YELLOW: Settings OK for PRD client, but not for all other clients.
RED: Settings not OK for PRD client.

Flags in table columns:
Modifiable
X - Production client is modifiable.
O - Non-production client is modifiable.
  - Client is not modifiable.

**Type**
P - Production client
D - Demo
E - Education
S - SAP Standard
C - Customizing
T - Test

**RED:**
**Evaluated Risk - High**
**YELLOW:**

**Evaluated Risk - Medium**

**GREEN:**

**Evaluated Risk - None**

Threats that arise with the possibility of development in production systems:
- Malfunction of system due to programs that have not been tested properly
- Unauthorized data access with modified or self-developed programs

**Flags in table columns**

**Modifiable**
X - Production client is modifiable
O - Non-production client is modifiable
  - Client is not modifiable

**Type**
P - Production client
D - Demo
E - Education
S - SAP Standard
C - Customizing
T - Test

**Recommendation:**
Set the Client Change Option to 'Not modifiable' in all clients in your production system.

**4.1.2.3 Users - Other Than System Administrators - Are Authorized to Change the System Change Option (0303)**

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).

**YELLOW/RED:** Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

**GREEN:**

**Evaluated Risk - None**

Development is possible in the production system by all of the following persons.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations,
depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE06 [as well as all relevant parameter transactions]
Object 2: S_CTS_ADMI with CTS_ADMFCT=INIT and CTS_ADMFCT=SYSC
Object 3: S_TRANSPRT with ACTVT=03 and TTYPE=* 

4.1.2.4 Users - Other Than System Administrators - Are Authorized to Change the Client Change Option (0304)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED: 
Evaluated Risk - High
GREEN:

Evaluated Risk - None
Development is possible in the productive client by all the following persons.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SCC4 [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02 DICBERCLS=SS
Object 3: S_TABU_CLI with CLIIDMAINT=* 
Object 4: S_ADMI_FCD with S_ADMI_FCD=T00

4.1.2.5 Clients with an Entry in T000 but Without Any User Data (0319)

Purpose
Clients with a T000 table entry but without any client data allow logons with the hard-coded user SAP* (unless this is prevented by a profile parameter).

Procedure
Check table USR02 (user master data) for all clients in T000 to see whether any such users exist.

Risk Rating
The rating is set automatically as follows:
GREEN: No client without data was found.
RED: At least one client without any user data was found.
RED: 
Evaluated Risk - High
GREEN:
Evaluated Risk - None
System access with hardcoded SAP* user in new clients.
Recommendation:
In table T000, delete all clients that contain no data.
4.1.2.6 Users - Other Than System Administrators - Are Authorized to Create New Clients (0305)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - High**
**GREEN:**

**Evaluated Risk - None**
Creating a new client means that logons are permitted with the hard-coded user SAP* unless this is prevented by a profile parameter.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
1. Object 1: S_TCODE with TCD=SCC4 [as well as all relevant parameter transactions]
2. Object 2: S_TABU_DIS with ACTVT=01 DICBERCLS=SS
3. Object 3: S_TABU_CLI with CLIIDMAINT=* 
4. Object 4: S_ADMI_FCD with S_ADMI_FCD=T000

4.1.2.7 Users Are Authorized to Delete Clients (0306)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - High**
**GREEN:**

**Evaluated Risk - None**
All the following users have the authority to delete any of your clients - including the production one. In addition, the default setting is that the T000 entry of the deleted client will not be deleted. Afterwards the hard-coded user SAP* is available with the well-known password PASS, unless this is prevented by a profile parameter.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to
check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SCC5 [as well as all relevant parameter transactions]
Object 2: S_TABU_CLI with CLIIDMAINT=X

4.1.2.8 Users Are Authorized to Development in the Production System (0307)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).

**YELLOW/RED:** Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
Threats that arise with the possibility of development in production systems:
- Malfunction of system due to programs that have not been tested properly
- Unauthorized data access with modified or self-developed programs

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE*
Object 2: S_DEVELOP with ACTVT=01 (create) or ACTVT=02 (change) and OBJTYPE=PROG

4.1.2.9 Users Are Authorized to Debug and Replace Field Values in the Production System (0308)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).

**YELLOW/RED:** Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
GREEN:

**Evaluated Risk - None**
Unauthorized access to data and functions, since any authorization checks can be bypassed with this authorization. In addition, you can change data during processing, which may lead to inconsistent results.

**Recommendation:**

---

<Service Name>, <Customer Name> <date of session>
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_DEVELOP with ACTVT=02 (change) and OBJTYPE=DEBUG

Note: If you do not want to disable development in your system, you have to exclude the OBJTYPE=DEBUG with ACTVT=02 from the profile and allow any other object type for S_DEVELOP. In this way, development and debugging with visualization is still possible. You can achieve this by linking 2 authorizations to the object S_DEVELOP. One with all object types (except for "DEBUG") and all activities, and another one for the object type DEBUG only and all activities (except for 02).

### 4.1.2.10 Users Are Authorized to Perform Customizing in the Production System (0309)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
- **RED**: Evaluated Risk - High
  System malfunction due to improperly tested Customizing.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD=SPRO [as well as all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=02 (change) and DICBERCLS=*

### 4.1.2.11 Users Are Authorized to Develop Queries in the Production System (0310)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
- **RED**:
Evaluated Risk - High
Data access in queries or by using ABAP programs within queries.
Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with (TCD=SQ00 or TCD=SQ01) [as well as all relevant parameter transactions]
Object 2: S_QUERY with ACTVT=02 (change)

4.1.2.12 Execution of CATTs and eCATTs is Not Prevented by Client Settings (0311)

Purpose
To disable the execution of CATT and eCATT in a PRD system to prevent unauthorized data transfer into the SAP system.

Procedure
In table T000, the system checks whether CCIMAILDIS contains blanks only. This check can be done manually with transaction SCC4: For all clients, check that the option 'Restrictions when starting CATT and eCATT' is set to 'eCatt and CATT not allowed'.

Risk Rating
The rating is set automatically as follows:
GREEN: Execution of CATT and eCATT is not allowed.
YELLOW: At least one client was found where execution of CATT and eCATT is allowed.

Flags in table columns:
CATTs allowed
X - CATTs and eCATTs allowed.
- CATTs and eCATTs not allowed.

Type
P - Production client
D - Demo
E - Education
S - SAP Standard
C - Customizing
T - Test

YELLOW:

Evaluated Risk - Medium
Unauthorized data transfer into the SAP system. In addition, the system could be rendered unstable if testing takes place during production operation. CATTs and eCATTs are very useful tools, but use them in the development and test environment only.

Flags in table columns
CATTs allowed
X - CATTs and eCATTs allowed
- CATTs and eCATTs not allowed

Type
P - Production client
D - Demo
E - Education
S - SAP Standard
C - Customizing
T - Test

Recommendation:
Disable the execution of CATTs and eCATTs, at least in the production client.
4.1.2.13 Users Are Authorized to Execute CATTs in the Production System (0312)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
- **YELLOW**:

Evaluated Risk - Medium
GREEN:

Evaluated Risk - None
Unauthorized data transfer into the SAP system.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE with TCD=SCAT [as well as all relevant parameter transactions]
- Object 2: S_DEVELOP with ACTVT=16 and OBJTYPE=SCAT

4.1.2.14 Users Are Authorized to Execute eCATTs in the Production System (0313)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
- **YELLOW**:

Evaluated Risk - Medium
GREEN:

Evaluated Risk - None
Unauthorized data transfer into the SAP system.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE with TCD=STWB_WORK or SECATT [as well as all relevant parameter transactions]
4.1.2.15 SAPgui User Scripting Is Enabled (0314)

**Purpose**
To check whether SAP GUI user scripting is enabled. SAP GUI user scripting does not exclude sensitive data, which means that actions are logged, for example, when creating a new user or changing a user's password.

SAP GUI user scripting is available as of SAP GUI Release 6.20, but as of R/3 Kernel Release 3.11 (see SAP Note 480149).

**Procedure**
Check the profile parameter sapgui/user_scripting. The return value is either FALSE (default) or TRUE.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN:** The parameter is set to FALSE or does not exist.
- **YELLOW:** The parameter is set to TRUE.

**Evaluated Risk - Medium**
As of SAP GUI 6.20, SAP supports this new parameter for all SAP R/3 releases as of Kernel Release 3.11. This parameter enables you to log your front-end activities. There is the possibility of misuse as it is possible to record sensitive data, for example when creating a new user or changing a user's password.

**Recommendation:**
Omit the parameter sapgui/user_scripting or set it to FALSE.
For further information, please refer to SAP Note 480149.

4.1.2.16 Users Are Authorized to Use the Legacy Migration Workbench (0315)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED:** Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - Medium**
**GREEN:**
**Evaluated Risk - None**
With LSMW it is possible to develop ABAP coding, even in a closed system without any development authorizations.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with LSMW [as well as all relevant parameter transactions]
Object 2: B_LSMW with TCD = LSMW and ACTVT = 02 or 16 or 36
Object 3: B_LSMW_PRO with PROJECT = *

4.1.2.17 Table Logging Is Not Enabled Sufficiently (0316)

**Purpose**
To check whether table auditing is enabled. Without table auditing, changes to customizing tables cannot be tracked.

**Procedure**
Check the profile parameter rec/client. The return value is a list of clients separated by commas or ALL.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN:** The parameter is set to ALL (all clients).
- **YELLOW:** The parameter is set to the productive client.
- **RED:** The parameter is not set or is blank.

**Evaluated Risk - High**
Recommendation:
Make sure that the profile parameter rec/client is set at least to your production client, or clients separated by commas, or even better, to ALL.

**YELLOW:**
Recommendation:
Set the profile parameter rec/client to ALL.
Lack of information for tracking unauthorized changes to Customizing.

4.1.2.18 Table Logging Is Not Enabled for Import (0317)

**Purpose**
To check whether table auditing is enabled for import into the production client. Without table auditing, changes to customizing tables cannot be tracked.

**Procedure**
Check the parameter recclient in file TPPARAM. Values are listed in SAP Note 84052.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN:** The parameter is set to ALL (all clients) or at least to the production client.
- **YELLOW:** The parameter is not maintained.

**Evaluated Risk - Medium**
Lack of information for tracking unauthorized changes to Customizing.
Recommendation:
Maintain the transport parameter recclient in STMS in the transport file, for example TP_DOMAIN_[sid].PFL, TPPARAM. Set it to ALL or at least set it to the production client.
For further information, please refer to SAP Note 84052.

4.1.2.19 Users Are Authorized to Modify the Table Logging Flag for Tables (0318)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN:** No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.

YELLOW:

Evaluated Risk - Medium

GREEN:

Evaluated Risk - None

Lack of information for tracking unauthorized changes to Customizing.

Recommendation:

Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:

Object 1: S_TCODE with TCD=SE11 or TCD=SE13 [as well as all relevant parameter transactions]
Object 2: S_DEVELOP with ACTVT=02 and OBJTYPE=TABT

4.1.3 Development

4.1.3.1 Development Sources Are Not Scanned for Critical Statements (0335)

Purpose

To find out whether the customer is aware that a new function is available as of 6.10: the Code Inspector. This program must be run on a regular basis.

Procedure

Ask customers in the questionnaire whether they know about the new function, and create the result here automatically.

Risk Rating

The rating is set automatically as follows:

GREEN: Code Inspector is used.
YELLOW: Code Inspector is not used.

YELLOW:

Evaluated Risk - Medium

GREEN:

Evaluated Risk - None

Coding might contain certain statements (listed as "Critical Statements" in the Code Inspector results) that are critical to security or endanger program stability.

Examples include:

- INSERT REPORT (ABAP command)
- EDITOR-CALL FOR REPORT (ABAP command)
- DELETE_USER_ON_DB (function module)
- BAPI_USER_* (function modules)

Recommendation:

Run the Code Inspector on a regular basis. The Code Inspector is available, along with some security checks, as of SAP Web AS 6.10.

4.1.3.2 Development Keys Exist in the Productive System (0338)

Purpose

To find users who have more authorizations than they need to perform their tasks.

Procedure

Check which users have authorization to start all reports by using transactions SA38 and SE38, for example.

Risk Rating

The rating is set automatically.
GREEN: Only key users can use SA38, SE38, and so on.
RED: Additional users have authorization to start reports by using SA38, SE38, and so on.
YELLOW:

**Evaluated Risk - Medium**
The users listed have a development key in the production system in table DEVACCESS. Together with the corresponding authorization, these users are allowed to develop directly in the production system.

### 4.1.4 Transport Control

#### 4.1.4.1 Users - Other Than Transport Administrators - Are Authorized to Change the TMS Configuration (0341)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
- **RED**: Evaluated Risk - High

Inconsistencies due to incorrectly configured CTS.

**Recommendation:**
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
- **Object 1:** S_TCODE with TCD = STMS [as well as all relevant parameter transactions]
- **Object 2:** S_CTS_ADMI with CTS_ADMFCT = TABL

#### 4.1.4.2 Users - Other Than Transport Administrators - Are Authorized to Start Imports to Production (0342)

**Purpose**
To find users who have more authorizations than they need to perform their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN**: No users found with surplus authorizations (except those specified in the questionnaire).
- **YELLOW/RED**: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
- **RED**: Evaluated Risk - High

**GREEN**: Evaluated Risk - None

Misuse of CTS (Change and Transport System) to import insecure programs. Inconsistencies due to incorrect usage of CTS.
Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=STMS [as well as all relevant parameter transactions]
Object 2: S_CTS_ADMI with CTS_ADMFCT=IMPA or CTS_ADMFCT=IMPS

4.1.4.3 Users - Other Than Transport Administrators - Are Authorized to Create and Release Transports (0343)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED: Evaluated Risk - High
the Change and Transport System (CTS) has been used incorrectly to export tables with sensitive data.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SE01 SE09 SE10 [as well as all relevant parameter transactions]
Object 2: S_TRANSPRT with ACTVT=01, 03 and 43 TTYPE=DTRA and TASK

4.1.4.4 Users Are Authorized to Approve Transports (0346)

Purpose
To find users who have more authorizations than they need to perform their tasks. The evaluated users in this check are only a risk in QA systems, as transaction STMS_QA does not work in other systems. We assume, however, that the authorizations are similar in production systems and QA systems.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED: Evaluated Risk - High
the Change and Transport System (CTS) has been used incorrectly to export tables with sensitive data.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SE01 SE09 SE10 [as well as all relevant parameter transactions]
Object 2: S_TRANSPRT with ACTVT=01, 03 and 43 TTYPE=DTRA and TASK

Import of programs that have not been tested properly.
Note: This check should normally run in the Quality System. We assume that if the users
have these authorizations in the Productive System, they also have them in the Quality System.

Recommendation: Check the roles and profiles of the users in your QA system that are evaluated by this check. Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=STMS_QA [as well as all relevant parameter transactions]
Object 2: S_CTS_ADMI with CTS_ADMFCT=QTEA

4.1.4.5 Users - Other Than Transport Administrators - Are Authorized to Apply Patches (0363)

Purpose
To find users who have more authorizations than they need to perform their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found with surplus authorizations (except those specified in the questionnaire).
YELLOW/RED: Multiple users with surplus authorizations were found. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
GREEN:
Evaluated Risk - None
System malfunction after import of patches. Functions were not tested properly.

Recommendation:
Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SPAM [as well as all relevant parameter transactions]
Object 2: S_TRANSPRT with TTYPE='PATC'

4.1.4.6 Transports Are Not Scanned for Viruses (0348)

Purpose
To avoid the import of non-secure programs by scanning the transports for viruses.

Procedure
Ask customers whether they scan their transports.

Risk Rating
No rating for this check. Customers can see how to scan their transports by reading SAP Note 521087.

YELLOW:

Recommendation:
Currently, transports into your system are not scanned automatically to avoid the import of non-secure programs. However, SAP provides a function for scanning the transports.
Review SAP Note 521087 for a description of how to set up a virus scanner for transport files, as these files are normally stored in a proprietary and compressed SAP format.

4.1.4.7 Program Versioning During Import is Not Enabled (0349)

**Purpose** To check whether versioning is performed in the DEV system where the changes are made. By setting the TP parameter VERS_AT_IMP to the value ‘ALWAYS’, a version is created after it is imported into the PRD system. This is sometimes required by auditors.

**Procedure** This can also be done manually by checking in transaction STMS whether the value for the PRD system is set to VERS_AT_IMP='ALWAYS' in the tpparam file.

**Risk Rating** The rating is set automatically as follows:
- GREEN: Versioning is enabled.
- YELLOW: Versioning is disabled.

**Evaluated Risk - Medium**

Recommendation:
Enable versioning in the Productive (PRD) system by setting the transport parameter VERS_AT_IMP to the value 'ALWAYS'. This is often requested by auditors.
5 SC_USERAUTH - SC User authorization checks

5.1 User Authorization

5.1.1 User Management

5.1.1.1 Users - Other Than the User Administrators - Are Authorized to Maintain Users (0002)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
Only user administrators should be authorized to create users.
You have to prevent users gaining unauthorized system access by using another user's account and also prevent interfaces malfunctioning if the interface user becomes invalid.
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SU01, TCD=OIBB, TCD=OOUS, TCD=OPF0, TCD=OPJ0, or TCD=OVZ5 [and all relevant parameter transactions]
Object 2: S_USER_GRP with ACTVT <> 03 (display) and ACTVT <> 08 (displ. change documents) and ACTVT <> SPACE

5.1.1.2 User Administrators Are Authorized to Change Their Own UserMaster Record (0003)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
YELLOW:
SC_USERAUTH - SC User authorization checks

**Evaluated Risk - Medium**
Avoid unauthorized maintenance of user accounts and assignment of authorizations.
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.
Authorization object:
S_USER_GRP with ACTVT=02 (change) CLASS = <same as assigned to the user administrator>

**5.1.1.3 User Administrators Are Allowed to Maintain Users of Any Group (0004)**

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.
RED:

**Evaluated Risk - High**

**YELLOW:**

**Evaluated Risk - Medium**
If user administration is segregated, prevent unauthorized maintenance of users who belong to a user group that the decentralized user administrator is not in charge of.
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.
Authorization Objects:
Object 1: S_TCODE with TCD = SU01 or TCD = OIBB or TCD = OOUS or TCD = OPF0 or TCD = OPJ0 or TCD = OVZ5 [as well as all relevant parameter transactions]
Object 2: S_USER_GRP with ACTVT = 02 (change) CLASS = *

**5.1.1.4 Users Are Not Assigned to User Groups (0005)**

**Purpose**
(Only if user administration is segregated.)
To check for unauthorized maintenance of users, who belong to a user group that the decentralized user administrator is not in charge of.

**Procedure**
The system checks which users do not belong to a user group.

**Risk Rating**
The rating is set automatically as follows.
GREEN: Up to 1% of users do not belong to a user group.
YELLOW: Between 1% and 5% of users do not belong to a user group.
RED: More than 5% of users do not belong to a user group.
RED:

**Evaluated Risk - High**
Recommendation: Add the users found to the appropriate user group.
YELLOW:
Evaluated Risk - Medium
Recommendation: Add the users found to the appropriate user group.
If user administration is segregated, prevent the unauthorized maintenance of users who
belong to a user group that the decentralized user administrator is not in charge of.
Users without a user group can be maintained by any user administrator.
Consider using segregated user administration, if not already in place. We recommend you
use dedicated superuser administrators, especially for standard users such as SAP* and
DDIC.

5.1.1.5 User Data Is Incomplete (0006)
Purpose
To check whether there is a lack of information for identifying or notifying users.
Procedure
The system checks for which users the address is not maintained (At least the name of the
user must exist).
Risk Rating
The rating is set automatically as follows:
GREEN: Up to 10% of users do not have an address.
YELLOW: More than 10% of users do not have an address.
YELLOW:
Evaluated Risk - Medium
Recommendation: Maintain the address of the users found.
Try to ensure you have sufficient information for identifying/notifying users.

5.1.1.6 User Master Data Is Not Regularly Synchronized with a Corporate LDAP
Directory (0007)
Purpose
To provide a function for synchronizing all the user master data from a global directory. This
feature is advantageous to the customer.
Procedure
The system checks whether the report RSLDAPSYNC_USER is scheduled on a regular
basis.
Risk Rating
No rating. Information is provided if synchronization is not currently active.
Show: No synchronization report is scheduled.
Skip: A synchronization report has already been scheduled.
YELLOW:
User master data can be synchronized with a corporate directory to avoid inconsistent data.
Recommendation: If you use a corporate directory, schedule the report
RSLDAPSYNC_USER on a regular basis. This ensures that all user master data is replicated
from this corporate directory and is always synchronized. Otherwise the data would not be
synchronized as it is stored redundantly.

5.1.1.7 Users with Authorizations for User and Role/Profile/Authorization
Maintenance (0008)
Purpose
To finds users who have more authorizations than they need for their tasks.
Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.
Risk Rating
The rating is set automatically as follows, but does not always include all three possible
values (GREEN/YELLOW/RED):
GREEN: No users found (except those specified in the questionnaire) who have surplus
authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

User and role maintenance must be segregated so that user administrators cannot change their own authorizations.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Remark: All users are listed who have authorization for check 0073, 0074, 0077, 0080, or 0081 (role and profile management in a production system) and who are also user managers (check 0002).

### 5.1.1.8 Reference Users Are Used (0011)

**Purpose**
To check whether broad authorizations are indirectly assigned by means of reference users.

**Procedure**
For each client, evaluate the reference users and the users that use the reference user.

**Risk Rating**
None

YELLOW:
Avoid broad authorizations that are assigned indirectly by means of reference users.

Only use reference users in Internet scenarios to assign roles to users who need the same authorizations.

Do not use this as a general technique for assigning roles.

SUIM reports do not consider authorizations that are assigned by means of reference users.

### 5.1.1.9 Usage of 'Normal' Users as Reference Users Is Not Prohibited (0012)

**Purpose**
To check whether broad authorizations are indirectly assigned by using reference users.

**Procedure**
Check whether the customizing switch REF_USER_CHECK=E is set in the PRGN_CUST table.

**Risk Rating**
The rating is set automatically.

GREEN: Customizing switch is set.

RED: Customizing switch is not set.

**RED:**

**Evaluated Risk - High**

Recommendation: Avoid use of 'normal' users as reference users by setting a customizing switch.

For more information, see SAP Note 513694.

### 5.1.1.10 Users - Other Than User Administrators - Are Authorized to Access Tables with User Data (0013)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED): 

GREEN: No users found (except those specified in the questionnaire) who have surplus
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
Avoid dictionary attacks on passwords stored in table USR02.
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE16, TCD=SE16N, or TCD=SE17 [and all relevant parameter transactions]
Object 2: S_TABU_DIS with DICBERCLS=SC ACTVT=03

5.1.1.11 Users - Other Than User Administrators - Are Authorized to Call Function Modules for User Admin (0019)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.

YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
Only user administrators should have authorizations to maintain users. Besides user maintenance in transaction SU01, users can be changed by calling function modules.
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE37 [and all relevant parameter transactions]
Object 2: S_DEVELOP with OBJTYPE=FUGR ACTVT=03 OBJNAME=SUSB RSUSR002 OR
Object 1: S_TCODE with TCD=SE37 [and all relevant parameter transactions]
Object 2: S_DEVELOP with OBJTYPE=FUGR ACTVT=03 OBJNAME=SU_USER
Object 3: S_USER_GRP with ACTVT=01 (create), ACTVT=02 (change), or ACTVT=06 (delete)

Remark for Release 6.40: As of Basis Release 6.40, ACTVT=16 is needed instead of ACTVT=03 for object S_DEVELOP in order to execute a function in SE37. If you are using a system with Basis Release 6.40 and a plug-in ST-A/PI_01E* or older, too many users might appear for this check.
5.1.2 Super Users

5.1.2.1 Users Have Nearly All Authorizations (0023)

**Purpose**
To check whether the customer allows broad system access to users who have too many authorizations.

**Procedure**
Search for users that have full access to >80% of all authorization objects (" field values).

**Risk Rating**
No rating for this check.

**YELLOW:**
No Evaluation
These users have more than 80% of all authorizations. They are "superusers."
Recommendation: Check which users have these authorizations and decide whether they really need them.

5.1.2.2 Unexpected Users Are Authorized to Change a Super User Accounts (0026)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found (except those specified in the questionnaire) who have surplus authorizations.

**YELLOW/RED:** Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**
Evaluated Risk - High
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SU01, TCD=OIBB, TCD=OOUS, TCD=OPF0, TCD=OPJ0, or TCD=OVZ5 [and all relevant parameter transactions]
Object 2: S_USER_GRP with ACTVT=02 (change) or ACTVT=05 and CLASS=SUPER

5.1.2.3 Users with the most Full Access Authorizations (* Field Values) (0027)

**Purpose**
To check whether the customer allows broad system access to users who have too many authorizations.

**Procedure**
Find 20% (maximum of 30) of all users that have full access for most authorization objects ("***" as field value).

**Risk Rating**
No risk rating for this check. The user list is displayed for information purposes only.

**GREEN:**
These users (max. 30 users or max. 20% of all users) have been granted the most authorization objects in your system. (They have the most wildcards "***" in the authorization objects of their user profiles.) This is merely for your information and is not necessarily critical.
You should check whether these users have accumulated rights (by moving to a new department, for example).

5.1.2.4 Users with the most Roles (0028)

**Purpose**
To check whether the customer allows broad system access to users who have too many authorizations.

**Procedure**
Find 20% (maximum of 30) of all users who have most roles (at least 50).

**Risk Rating**
No risk rating for this check. The user list is displayed for information purposes only.

**GREEN:**
These users (max. 30 users or max. 20% of all users) have the most roles in your system. This is merely for your information and is not necessarily critical. You should check whether these users have accumulated rights (by moving to a new department, for example). Only users with 50 or more roles have been taken into consideration.

5.1.2.5 20% or max 30 of All Users That Have for the most Profiles (0029)

**Purpose**
To check whether the customer allows broad system access to users who have too many authorizations.

**Procedure**
Find 20% (maximum of 30) of all users that have most profiles.

**Risk Rating**
No risk rating for this check. The user list is displayed for information purposes only.

**GREEN:**
These users (max. 30 users or max. 20% of all users) have the most profiles in your system. This is merely for your information and is in no way critical. You should check whether these users have accumulated rights (by moving to a new department, for example). Only users with 50 or more profiles have been taken into consideration.

5.1.2.6 Users with Profile SAP_NEW (0031)

**Purpose**
To find users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:**
No users found (except those specified in the questionnaire) who have surplus authorizations.

**YELLOW/RED:**
Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
The profile SAP_NEW cumulates a lot of authorizations. Please use only the subprofile(s) of SAP_NEW corresponding to your last release change. You should then update your own profiles as soon as possible and remove the SAP_NEW profile.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.
5.1.3 Standard Users

5.1.3.1 User SAP* has the default password in some clients (0041)

Purpose
To check for misuse of standard user.
It is recommended to disable SAP* and use an alternative superuser instead of the well-known SAP*.

Procedure
The system checks the password of the SAP* user.

Risk Rating
The rating is set automatically as follows:
GREEN: Password changed or password authentication disabled.
RED: Standard password not changed.
RED:

Evaluation Risk - High
Recommendation: Change the standard password 06071992 of user SAP*.

5.1.3.2 Not all profiles are removed from user SAP* (0042)

Purpose
To check for misuse of the standard user.

Procedure
The system checks the profiles of the SAP* user.

Risk Rating
The rating is set automatically as follows:
GREEN: No profile assigned.
YELLOW: A profile is assigned to SAP*.
YELLOW:

Evaluation Risk - Medium
Recommendation: Remove the profile(s) from the SAP* user and create another superuser to be used as an emergency user.
Possible table values:
"": SAP* has no profiles
"X": Profile SAP_ALL is used
"O": Another profile is used.

5.1.3.3 User SAP* is neither locked nor expired (0043)

Purpose
To avoid misuse of standard user.

Procedure
The system checks the lock or expiration date of the SAP* user.

Risk Rating
The rating is set automatically.
GREEN: User locked or expiration date set.
RED: User neither locked nor expiration date set.
YELLOW:

Evaluation Risk - Medium
Recommendation: The user SAP* is unlocked in at least one client. To prevent the usage of SAP*, lock the user account or set an expiration date. Do not delete SAP*.

5.1.3.4 User SAP* is not assigned to the user group SUPER (0044)

Purpose
To avoid misuse of standard user. Users without a user group can be maintained by any user administrator.

Procedure
The system checks the user group of user SAP*. 
Risk Rating
The rating is set automatically as follows:
GREEN: SAP* is assigned to user group SUPER.
YELLOW: SAP* is assigned to any other user group or to no user group at all.
Background: Superusers must be maintained by dedicated user administrators only.
YELLOW:

Evaluated Risk - Medium
Recommendation: Assign SAP* to user group SUPER so that the user can be maintained by certain user administrators only.

5.1.3.5 User SAP* has been deleted at least in one client (0045)
Purpose
To avoid misuse of standard user. If user SAP* is deleted, access with hard-coded user SAP* is possible.
Procedure
The system checks the existence of SAP* in all clients.
Risk Rating
The rating is set automatically as follows:
GREEN: SAP* exists in all clients.
RED: SAP* has been removed in at least one client.
RED:
Evaluated Risk - High
Recommendation: User SAP* has been deleted in at least one client. Do not delete SAP* in any client. If you do so, the usage of the hard-coded user SAP* is enabled if it is not prohibited by the profile parameter "login/no_automatic_user_sapstar".

5.1.3.6 Usage of the hard coded user SAP* is not disabled (0046)
Purpose
To avoid misuse of standard user. If user SAP* is deleted, access with hard-coded user SAP* and password PASS is possible. This can be prohibited by using a profile parameter.
Procedure
The profile parameter login/no_automatic_user_sapstar is checked. Return value is 0 or 1.
Risk Rating
The rating is set automatically as follows:
GREEN: The value is 1 (which means that the hard-coded SAP* user cannot be used).
RED: The value is 0.
RED:
Evaluated Risk - High
Recommendation: Set the profile parameter "login/no_automatic_user_sapstar" to 1.
Note: The user SAP* is needed for the client copy. Therefore, the parameter has to be changed back to 0 before the client copy is started - at least for the application server that you want to use for logging on to the new client.

5.1.3.6.1 Usage of the hard coded user SAP* is not disabled (0046)

5.1.3.7 User SAP**s activities are not logged in the Security Audit Log (0047)
Purpose
To check that activities of the user SAP* are recorded in the Security Audit Log to ensure that enough information is available to track security incidents.
Procedure
The system checks the customizing of the Security Audit Log.
Risk Rating
The rating is set automatically.
GREEN: At least the unsuccessful activities of SAP* in all clients are logged in the Security Audit Log.
SC_USERAUTH - SC User authorization checks

**YELLOW**: The Security Audit Log is not enabled for SAP* or only the successful activities are logged.

**YELLOW**: 

**Evaluated Risk - Medium**
Recommendation: Log the successful and (at least) the unsuccessful activities for the user SAP* in the Security Audit Log.
Possible table values:
"": No events are logged.
"S": Successful events are logged.
"U": Unsuccessful events are logged.

**5.1.3.8 User DDIC has the default password in some clients (0048)**

**Purpose**
To avoid misuse of standard user.

**Procedure**
The system checks the password of the SAP standard user "DDIC".

**Risk Rating**
The rating is set automatically as follows:
**GREEN**: Password changed or password authentication disabled.
**RED**: Standard password not changed.

**Background**:
The DDIC user is necessary for running transports (batch job RDDIMPDP is scheduled for the user account of DDIC) and therefore can neither be locked nor deleted.
DDIC needs SAP_ALL.

**RED**: 

**Evaluated Risk - High**
Recommendation: Change the standard password 19920706 of the SAP standard user DDIC.

**5.1.3.9 User DDIC Is Not Assigned to the User Group SUPER (0049)**

**Purpose**
To avoid misuse of the standard user. Users without a user group can be maintained by any user administrator.

**Procedure**
The system checks the user group of user DDIC.

**Risk Rating**
The rating is set automatically as follows:
**GREEN**: DDIC is assigned to the user group SUPER.
**YELLOW**: DDIC is assigned to any other user group or to no group at all.
**Background**:
Superusers must be maintained by dedicated user administrators only.

**YELLOW**: 

**Evaluated Risk - Medium**
Recommendation: Assign the SAP standard user DDIC to the user group SUPER so that the user can be maintained by certain user administrators only.

**5.1.3.10 User DDIC's activities are not logged in the Security Audit Log (0050)**

**Purpose**
To check whether activities of DDIC are recorded in the Security Audit Log to ensure that information on security incidents can be tracked.

**Procedure**
The system checks the customizing of the Security Audit Log.

**Risk Rating**
The rating is set automatically as follows:
**GREEN**: At least the unsuccessful activities of DDIC in all clients are logged in the Security
Audit Log.

YELLOW: Security Audit Log is not enabled for the user DDIC.

YELLOW:

**Evaluated Risk - Medium**
Recommendation: Log the successful and (at least) the unsuccessful events for the user DDIC in the Security Audit Log.

5.1.3.11 User SAPCPIC has the default password in some clients (0051)

**Purpose**
To avoid misuse of standard user.

**Procedure**
The system checks the password of SAPCPIC.

**Risk Rating**
The rating is set automatically as follows:
GREEN: Password changed or password authentication disabled.
RED: Standard password not changed.

YELLOW:

**Evaluated Risk - Medium**
Recommendation: Log the successful and (at least) the unsuccessful events for the user DDIC in the Security Audit Log.

5.1.3.11 User SAPCPIC has the default password in some clients (0051)

**Purpose**
To avoid misuse of standard user.

**Procedure**
The system checks the password of SAPCPIC.

**Risk Rating**
The rating is set automatically as follows:
GREEN: Password changed or password authentication disabled.
RED: Standard password not changed.

RED:

**Evaluated Risk - High**
Recommendation: Change the standard password ADMIN of user SAPCPIC.

5.1.3.12 User SAPCPIC Is Neither Locked nor Expired (0052)

**Purpose**
To avoid misuse of standard user.

**Procedure**
The system checks the lock or expiration date of SAPCPIC.

**Risk Rating**
The rating is set automatically as follows:
GREEN: User locked or expiration date set.
RED: User neither locked nor expiration date set.

YELLOW:

**Evaluated Risk - Medium**
Recommendation: To prevent the usage of SAPCPIC, lock the user account or set an expiration date.

5.1.3.13 User SAPCPIC Not Assigned to the Group SUPER (0053)

**Purpose**
To avoid misuse of standard user. Users without a user group can be maintained by any user administrator.

**Procedure**
The system checks the user group of user SAPCPIC.

**Risk Rating**
The rating is set automatically as follows:
GREEN: SAPCPIC is assigned to user group SUPER.
YELLOW: SAPCPIC is assigned to any other user group or to no user group at all.

**Background:** Superusers must be maintained by dedicated user administrators only.

YELLOW:

**Evaluated Risk - Medium**
Recommendation: Assign SAPCPIC to user group SUPER so that the user can be maintained by certain user administrators only.

Possible table values:

- "": Assigned to user group SUPER
- "X": Not assigned to user group SUPER
- "O": Assigned to another user group
5.1.3.14 User SAPCPIC Has More Authorizations Than Required (0054)

**Purpose**
To avoid misuse of standard user.

**Procedure**
The system checks the profiles of the SAP standard user SAPCPIC.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: SAPCPIC has the S_A.CPIC profile only.
- **YELLOW**: More profiles are assigned than S_A.CPIC.
- **RED**: Profile SAP_ALL is assigned.

**Evaluated Risk - High**
Recommendation: Remove all profiles other than S_A.CPIC from user SAPCPIC.

**Possible table values:**
- "": User SAPCPIC has profile S_A.CPIC
- "O": User SAPCPIC has a profile other than S_A.CPIC
- "X": User SAPCPIC has SAP_ALL.

**Evaluated Risk - Medium**
Recommendation: Remove all profiles other than S_A.CPIC from user SAPCPIC.

5.1.3.15 User SAPCPIC’s activities are not logged in the Security Audit Log (0055)

**Purpose**
To check that activities of SAPCPIC are recorded in the Security Audit Log to ensure that information on security incidents can be tracked.

**Procedure**
The system checks the customizing of the Security Audit Log.

**Risk Rating**
The rating is set automatically as follows.
- **GREEN**: The unsuccessful activities of SAPCPIC in all clients are logged in the Security Audit Log.
- **YELLOW**: The Security Audit Log is not enabled or only successful events are logged.

**Evaluated Risk - Medium**
Recommendation: Log at least the unsuccessful events for the user SAPCPIC in the Security Audit Log.

5.1.3.16 User EARLYWATCH has the default password (0056)

**Purpose**
To avoid misuse of standard user.

**Procedure**
The system checks the password of user EARLYWATCH.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: Password changed or password authentication disabled.
- **RED**: Standard password not changed.

**Evaluated Risk - High**
Recommendation: Change the standard password SUPPORT of the user EARLYWATCH.

5.1.3.17 User EARLYWATCH Is Not Assigned to User Group SUPER (0058)

**Purpose**
To avoid misuse of the standard user. Users without a user group can be maintained by any user administrator.
**Procedure**
The system checks the user group of user EARLYWATCH.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: EARLYWATCH is assigned to user group SUPER.
- **YELLOW**: EARLYWATCH is assigned to any other user group or to no group at all.

**Background**: Superusers must be maintained by dedicated user administrators only.

**Evaluated Risk - Medium**
Recommendation: Assign the SAP standard user EARLYWATCH to the user group SUPER so that the user can be maintained by certain user administrators only.

5.1.3.18 User EARLYWATCH Has More Authorizations Than Required (0059)

**Purpose**
To avoid misuse of standard user EARLYWATCH.

**Procedure**
The system checks the profiles of user EARLYWATCH.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: Only the profile S_TOOL_EX_A is assigned.
- **YELLOW**: Profile other than S_TOOL_EX_A is assigned.

**Evaluated Risk - Medium**
Recommendation: Remove all profiles except S_TOOL_EX_A from the EARLYWATCH user.

5.1.3.19 User EARLYWATCH’s activities are not logged in the Security Audit Log (0060)

**Purpose**
To check that activities of user EARLYWATCH are recorded in the Security Audit Log to ensure that information for security incidents can be tracked.

**Procedure**
The system checks the customizing of the Security Audit Log.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: All unsuccessful activities of EARLYWATCH in all clients are logged in the Security Audit Log.
- **YELLOW**: The unsuccessful activities of EARLYWATCH are not logged.

**Evaluated Risk - Medium**
Recommendation: Log at least the unsuccessful events for user EARLYWATCH in the Security Audit Log.

5.1.3.20 User TMSADM has the default password in some clients (0063)

**Purpose**
The check prevents misuse of SAP standard user TMSADM.

**Procedure**
The system checks whether the TMSADM user still has the standard password.

**Risk Rating**
The rating is set automatically as follows:
- **GREEN**: The TMSADM user does not have a standard password for any client.
- **YELLOW**: The TMSADM user has a standard password for at least one client.

**Evaluated Risk - Medium**
Recommendation: Change the standard password for the TMSADM user. (For clients other than client 000, you should delete the user instead.)
SC_USERAUTH - SC User authorization checks

SAP Note 1414256 describes a support tool for changing the password for the TMSADM user in all systems of the transport domain.
SAP Note 1552894 shows how to update the report RSUSR003 for showing the status of TMSADM user, too.

5.1.3.21 User TMSADM Exists in Clients Other Than Client 000 (0064)

**Purpose**
The check prevents misuse of SAP standard user TMSADM.

**Procedure**
The TMSADM user is required for client 000 only.
The system checks the existence of the TMSADM user for all clients except client 000.

**Risk Rating**
The rating is set automatically as follows:

**GREEN**: The TMSADM user does not exist for any client except client 000.

**YELLOW**: The TMSADM user exists for at least one client.

**YELLOW**: Evaluated Risk - Medium
Recommendation: Delete the TMSADM user for all clients except client 000.

5.1.3.22 User TMSADM has more authorizations than required (0065)

**Purpose**
To avoid misuse of the TMSADM standard user.

**Procedure**
The system checks the profiles of the TMSADM user.

**Risk Rating**
The rating is set automatically as follows:

**GREEN**: Only the S_A.TMSADM profile is assigned.

**YELLOW**: Profiles other than S_A.TMSADM are assigned.

**YELLOW**: Evaluated Risk - Medium
Recommendation: Remove all profiles from the TMSADM user except the S_A.TMSADM profile.

5.1.4 Role & Authorization Management

5.1.4.1 Users Are Authorized to Maintain Roles Directly in the Production System (0072)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN**: No users found (except those specified in the questionnaire) who have surplus authorizations.

**YELLOW/RED**: Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED**: Evaluated Risk - High
Roles, profiles, and authorizations must always be changed in the development system.
Therefore, authorizations for role and authorization maintenance do not need to be assigned in the productive system at all.
Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations,
depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=PFCG [and all relevant parameter transactions]
Object 2: S_USER_AGR with ACTVT=01 (create) or ACTVT=02 (change)

5.1.4.2 Users Are Authorized to Maintain Profiles Directly in the Production System (0073)

Purpose
To finds users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.

Evaluated Risk - High
Roles, profiles, and authorizations must always be changed in the development system. Therefore, authorizations for role and authorization maintenance do not need to be assigned in the productive system at all.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SU02 [and all relevant parameter transactions]
Object 2: S_USER_PRO with ACTVT=01 (create) or ACTVT=02 (change) or ACTVT=06 (delete).

5.1.4.3 Users Are Authorized to Maintain Authorizations Directly in the Production System (0074)

Purpose
To finds users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.

Evaluated Risk - High
Roles, profiles, and authorizations must always be changed in the development system. Therefore, authorizations for role and authorization maintenance do not need to be assigned in the productive system at all.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations,
depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SU03 [and all relevant parameter transactions]
Object 2: S_USER_AUT with ACTVT=01 (create) or ACTVT=02 (change)

5.1.4.4 Users Are Authorized to Call Function Modules for Authorization, Role and Profile Management (0087)

Purpose
To find users who have more authorizations than they need for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

GREEN: No users found (except those specified in the questionnaire) who have surplus authorizations.
YELLOW/RED: Multiple users with surplus authorizations found. The rating depends on the severity of this check.
RED: Evaluated Risk - High

Roles/profiles/authorizations can be maintained in PFCG, SU02, and SU03, and can also be changed by calling function modules of the groups SUSA, SUSC, SUSX, and SUSE. Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE37 [and all relevant parameter transactions]
Object 2: S_DEVELOP with OBJTYPE=FUGR and OBJNAME=PRGN and ACTVT=03

Remark: As of Basis Release 6.40, ACTVT=16 is required instead of ACTVT=03 for object S_DEVELOP in order to execute a function in SE37. If your system is on Basis Release 6.40, too many users might appear in this check.

Remark for Release 6.40: As of Basis Release 6.40, ACTVT=16 is needed instead of ACTVT=03 for object S_DEVELOP in order to execute a function in SE37. If you are using a system with Basis Release 6.40 and a plug-in ST-A/PI_01E* or older, too many users might appear for this check.

5.1.4.5 SAP Standard Roles Are Assigned to Users (0082)

Purpose
To check that predefined SAP roles are only used as a template. They should not be assigned to users. In some cases, it is recommended to use special, predefined roles or profiles.

Procedure
The system checks for standard SAP roles.

Risk Rating
The rating is set automatically as follows:

GREEN: No standard SAP roles are assigned to users.
YELLOW: A maximum of 5 standard SAP roles are assigned to users.
RED: More than 5 standard SAP roles are assigned to users.
RED: Evaluated Risk - High
Recommendation: Only use predefined SAP roles as templates. Do not assign them to users due to the number of authorizations assigned to standard SAP roles.

**YELLOW:**

**Evaluated Risk - Medium**
Recommendation: Only use predefined SAP roles as templates. Do not assign them to users due to the number of authorizations assigned to standard SAP roles.

### 5.1.4.6 SAP Standard Profiles Are Assigned to Users (0083)

**Purpose**
To check that predefined SAP profiles are only used as a template. They should not be assigned to users.

**Procedure**
The system checks for standard SAP profiles.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** No SAP standard profiles are assigned to users.

**YELLOW:** A maximum of 5 standard SAP profiles are assigned to users.

**RED:** More than 5 standard SAP profiles are assigned to users.

**RED:**

**Evaluated Risk - High**
Recommendation: Only use predefined SAP profiles as templates. Do not assign them to users due to the large number of authorizations assigned to standard SAP profiles.

**YELLOW:**

**Evaluated Risk - Medium**
Recommendation: Only use predefined SAP profiles as templates. Do not assign them to users due to the number of authorizations assigned to standard SAP profiles.

### 5.1.4.7 Inconsistent Assignment of Generated Profiles (0084)

**Purpose**
To check that generated profiles are not assigned directly to users; Roles should be used instead.

**Procedure**
The system checks for generated profiles that have been directly assigned.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** There are no directly assigned profiles.

**RED:** There are directly assigned profiles.

**RED:**

**Evaluated Risk - High**
Recommendation: Always assign generated profiles indirectly (never directly) in roles. Otherwise, a profile assignment can be deleted accidentally when users are compared using PFCG_TIME_DEPENDENCY.

### 5.1.4.8 Unused Roles Are Found (0086)

**Purpose**
To check whether the temporary assigned roles have been removed. To remove temporary assigned roles the report PFCG_TIME_DEPENDENCY must be scheduled. Ideally, this report should be executed every day.

**Procedure**
The system checks for temporary assigned roles that have not been removed.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** No unremoved temporary assigned roles exist that are out of date.

**RED:** Unremoved temporary assigned roles exist that are out of date.

**RED:**
SC_USERAUTH - SC User authorization checks

Evaluated Risk - High
Recommendation: To remove temporary roles, schedule the report
PFCG_TIME_DEPENDENCY. Ideally, this report should be executed every day.

5.1.4.9 Profiles on Long Time Locked Users (0089)

Purpose
To check whether users locked for a long period of time still have assigned profiles.

Procedure
The system checks for users locked for over 180 days and who still have assigned profiles.

Risk Rating
The rating is set automatically as follows:
GREEN: No unremoved temporary assigned roles exist that are out of date.
YELLOW: Unremoved temporary assigned roles exist that are out of date.

Recommendation: We found users that have been locked for at least 180 days still with assigned profiles in the marked clients. Remove profiles from users that have been locked for a long period of time (especially if they have left the company). Unlocking a user can give access to broad authorizations.

5.1.5 Authorizations

5.1.5.1 Authorization Checks Within Certain Transactions Are PartlyDisabled (0101)

Purpose
To inform the customer whether authorization checks are disabled in the system.

Procedure
The system checks whether there are entries in table USOBX_CD with selection CHNGIND='U', and whether the profile parameter auth/no_check_in_some_cases is set to "Y".

Risk Rating
No rating for this check. The customer is informed whether authority checks are disabled.
YELLOW:
You have defined disabled authorization checks within some transactions in transaction SU24. Also, the profile parameters "auth/no_check_in_some_cases" and "auth/object_disabling_active" are set to "Y", which means that there are disabled authority checks in your system.

5.1.5.2 Authorization Checks for Certain Authorization Objects Are Disabled (0103)

Purpose
To inform the customer whether authorization checks are disabled in the system.

Procedure
The system checks whether there are entries in table TOBJ_OFF.
To be checked only if the following profile parameters are set:
- auth/no_check_in_some_cases=Y
- auth/object_disabling_active=Y
The check is set automatically as follows:

Risk Rating
No rating for this check. The customer is informed whether authorization checks are disabled.
YELLOW:
In transaction AUTH_SWITCH_OBJECTS, you have disabled authorization checks for certain authorization objects within any transaction. Also, the profile parameters "auth/no_check_in_some_cases" and "auth/object_disabling_active" are set to "Y". The authorization objects listed in the table are disabled in your system.
5.1.5.3 Users Are Authorized to Disable Authorization Checks Within Transactions (0102)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN:** No users found (except those specified in the questionnaire) who have surplus authorizations.
- **YELLOW/RED:** Multiple users with surplus authorizations found. The rating depends on the severity of this check.
- **RED:**

**Evaluated Risk - High**
No user should have authorizations to disable authorization checks for any transaction.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE=SU24 [and all relevant parameter transactions]
- Object 2: S_USER_GRP with ACTVT=* and CLASS=*  
- Object 3: S_DEVELOP with ACTVT=03 and OBJTYPE=SUSO

5.1.5.4 Users Are Authorized to Disable Authorization Checks Globally (0105)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
- **GREEN:** No users found (except those specified in the questionnaire) who have surplus authorizations.
- **YELLOW/RED:** Multiple users with surplus authorizations found. The rating depends on the severity of this check.
- **RED:**

**Evaluated Risk - High**
No user should have authorizations to disable authorization objects.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization Objects:**
- Object 1: S_TCODE=AUTH_SWITCH_OBJECTS [and all relevant parameter transactions]
- Object 2: S_USER_OBJ with ACTVT=02 (change)

5.1.5.5 Users Are Authorized to Call Any Transaction (0110)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.
Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found (except those specified in the questionnaire) who have surplus authorizations.

**YELLOW/RED:** Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

When all transactions are allowed to be started, access relies completely on authorization checks in the executed report.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization Object:**
Object S_TCODE with field TCD =*

5.1.5.6 Users Are Authorized to Delete an Authorization Check Before Transaction Start (0111)

**Purpose**
To finds users who have more authorizations than they need for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found (except those specified in the questionnaire) who have surplus authorizations.

**YELLOW/RED:** Multiple users with surplus authorizations found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

In transaction SE93, a basic authorization check can be maintained for every transaction. Deleting this authorization check could create security holes.

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the Authorization Info System (SUIM) to check the results. For this check we recommend that you examine the roles or profiles that include the authorization objects listed below.

**Authorization objects:**
Object 1: S_TCODE with TCD=SE93 [and all relevant parameter transactions]
Object 2: S_DEVELOP with OBJTYPE=TRAN and ACTVT = 02

5.1.5.7 Global Disabling of Authority Checks Is Not Prevented (0104)

**Purpose**
To avoid bypassing authorization checks.

**Procedure**
The system checks the profile parameter auth/object_disabling_active. The return value is 'Y', 'N', or blank.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** The value is 'N' or the table TOBJ_OFF is not empty
SC_USERAUTH - SC User authorization checks

**RED:** The value is 'Y' or blank, and the table TOBJ_OFF is not empty. This means that authorization checks can be globally deactivated, but the feature is not used.

**YELLOW:**

**Evaluated Risk - High**
Table TOBJ_OFF does not contain deactivated authorization objects but the profile parameter "auth/object_disabling_active" is set to "Y" nonetheless.
Recommendation: Set the profile parameter "auth/object_disabling_active" to "N". This means that authorization checks cannot be deactivated globally by users who have the appropriate authorization.

**5.1.5.8 Authority Check for Inbound RFC Connections Is Disabled (0106)**

**Purpose**
To avoid bypassing authorization checks.

**Procedure**
The system checks the profile parameter auth/rfc_authority_check. The return value is '0', '1', '2', or '9'.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** The value is > '0'.

**RED:** The value is '0'. This means that no authorization checks are performed for S_RFC in RFC calls.

**RED:**

**Evaluated Risk - High**
Recommendation: Set the profile parameter "auth/rfc_authority_check" to '1', '2', or '9' to perform authority checks for the authorization object S_RFC within RFC calls.

**5.1.5.8.1 Authority Check for Inbound RFC Connections Is Disabled (0106)**

**Purpose**
To avoid bypassing authorization checks.

**Procedure**
The system checks the profile parameter auth/rfc_authority_check. The return value is '0', '1', '2', or '9'.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** The value is > '0'.

**RED:** The value is '0'. This means that no authorization checks are performed for S_RFC in RFC calls.

**RED:**

**Evaluated Risk - High**
Recommendation: Set the profile parameter "auth/rfc_authority_check" to '1', '2', or '9' to perform authority checks for the authorization object S_RFC within RFC calls.

**5.1.5.9 Authority Check for Inbound tRFC Connections Is Disabled (0107)**

**Purpose**
To avoid bypassing authorization checks.

**Procedure**
The system checks the profile parameter auth/trfc_no_authority_check. The return value is '0' or '1'.

**Risk Rating**
The rating is set automatically as follows:

**GREEN:** The value is '0'.

**RED:** The value is '1'. This means that no authorization checks are performed for S_RFC in transactional RFC calls.

**RED:**

**Evaluated Risk - High**
Recommendation: Set the profile parameter "auth/trfc_no_authority_check" to '0'. This means that authorization checks for S_RFC are performed for transactional RFC calls.

5.1.5.10 Authority Check for Particular ABAP Elements Is Disabled (0108)

Purpose
To avoid bypassing authorization checks.

Procedure
The system checks the profile parameter auth/system_access_check_off. The return value is '0' or '1'.

Risk Rating
The rating is set automatically as follows:
GREEN: The value is '0'.
YELLOW: The value is '1'. This means that for certain ABAP elements the authorization checks can be deactivated (file operations, CPIC calls, calls to kernel functions, and so on).
YELLOW:
Evaluated Risk - Medium
Recommendation: Set the profile parameter "auth/system_access_check_off" to '0'.

5.1.5.11 Authority Check on S_TCODE Is Disabled (0109)

Purpose
To avoid bypassing authorization checks.

Procedure
The system checks the profile parameter auth/check/calltransaction. The return value is '0', '1', or '3'. The parameter can be used to switch off authorization checks on S_TCODE when the transaction is started within another transaction using CALL TRANSACTION statement. Currently, we recommend that you do not use 0 as we do not know how 3 works in live systems.

Risk Rating
GREEN: The value is '1'.
YELLOW: The value is '0' or blank. This means no additional authorization checks are performed for a second transaction call.
YELLOW:
Evaluated Risk - Medium
Recommendation: Set the profile parameter "auth/check/calltransaction" to '1'. This means that an authorization check on S_TCODE is performed when a transaction is called within another transaction.

For more information, see SAP Note 410622 at http://www.service.sap.com/~iron/fm/011000358700000431401997E/0410622.

5.1.5.12 Users Comparison After Role Change Is Not Run in a Timely Accurate Manner (0112)

Purpose
To avoid bypassing authorization checks.

Procedure
The system checks the profile parameter auth/new_buffering. The return value is between '2' and '5'.

Risk Rating
The rating is set automatically as follows:
GREEN: The value is '4'.
YELLOW: The value is '2' or '3'. This means that changes to the authorizations of a particular user do not take effect immediately, but only when the user next logs on.
YELLOW:
Evaluated Risk - Medium
Recommendation: Set the profile parameter "auth/new_buffering" to '4'. This means that changes to the authorizations of a user take effect immediately, and not only after the next logon.

5.1.5.12.1 Users Comparison After Role Change Is Not Run in a Timely Accurate Manner (0112)
6 SC_WEBAS - Web Application Server

6.1 Web Application Server

6.1.1 Internet Communication Framework (ICF)

6.1.1.1 Active ICF Services (0664)

**Purpose**
To ask the customer for unused active ICF services in Basis Release 6.10.

**Rating**
The check is not rated. It is only shown if the current Basis Release is 6.10.

**Background**
In Release 6.10, certain ICF services have been delivered in status active. If the customer does not use them, they should be deactivated.

**GREEN:**
Recommendation: With Basis Release 6.10, certain ICF services are delivered with the default status "Active." If you do not use these services, deactivate them in transaction SICF.

6.1.1.2 Unused ICF Services Are Activated (0652)

**Purpose**
To avoid system access with ICF services that are not in use.

**Procedure**
Check table ICFSERVICE for unused but active services. Exclude HTTP services that must be activated when using the SAP Web Dispatcher for load balancing.
- /sap/public/icman
- /sap/public/icf_info/*

**Risk Rating**
The rating is set automatically as follows:
**GREEN:** Only the necessary services are active.
**RED:** Additional services are active.

**Evaluated Risk - High**
At least one service is active but not in use.
System access with ICF services that are not in use.

6.1.1.3 ICF Service Can Be Called via Unsecured http Connection (0653)

**Purpose**
To avoid unsecured HTTP connection to any (active) ICF service possible that requires encrypted communication.

**Procedure**
First, check whether HTTPS plug-in is available, then scan table ICFSERVICE with selection PROTSEC=S.

**Risk Rating**
The rating is set automatically as follows:
**GREEN:** No unsecured communication to sensitive HTTP service possible.
**RED:** Unsecured communication to at least one HTTP service possible although secured communication required.

**Evaluated Risk - High**
Insecure HTTP communication is possible with at least one HTTP service, although secure communication is required.
Insecure communication with HTTP service that allows eavesdropping of sensitive communication data.

**6.1.1.4 Access to ICF Services Does Not Require Authorization for S_SICF (0654)**

**Purpose**
To check whether all (active) HTTP services require an authorization for S_SICF.

**Procedure**
Scan table ICFSERVICE with selection ICF_AUTH for all active HTTP services.

**Risk Rating**
The rating is set automatically as follows:

- **GREEN**: Authorization value maintained for all active HTTP services.
- **RED**: At least one active HTTP service without authorization value.

**Evaluated Risk - High**
At least one active HTTP service does not have an authorization value for S_SICF. Unauthorized access to ICF services.

**6.1.1.5 Users - Other Than System Administrators - Are Authorized to Activate ICF Services (0655)**

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

- **GREEN**: No users found (except specified in the questionnaire) with surplus authorizations.
- **YELLOW/RED**: Additional users found with surplus authorizations. The rating depends on the severity of this check.

**Evaluated Risk - High**
GREEN:

**Evaluated Risk - None**
Access to ICF services after unauthorized activation.

**Recommendation**: Use the Profile Generator (PFCG) to correct roles, and/or transactions SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the Authorization Info System (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

**Authorization objects**:
- Object 1: S_TCODE with TCD=SICF [and all relevant parameter transactions]
- Object 2: S_ADMI_FCD = PADM

**6.1.1.6 Users - Other Than System Administrators - Are Authorized to Access Table Authorization Group &NC& (0663)**

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

- **GREEN**: No users found (except specified in the questionnaire) with surplus authorizations.
YELLOW/RED: Additional users found with surplus authorizations. The rating depends on the severity of this check.

RED:

**Evaluated Risk - High**
Tables which are not assigned to a specific table authorization group (see transaction SE54 or Table TDDAT) are implicitly part of table authorization group &NC&. This table authorization group contains many tables including critical tables.

Example: Access to table ICFSERVICE using standard table maintenance tools like SE16 could be misused to find ICF services with anonymous access.

Therefore you should not give access to table authorization group &NC&. If you need access to specific tables you can either assign these tables to a different table authorization group or you can grant authorizations individually using authorization object S_TABU_NAM.

Recommendation: Use the Profile Generator (PFCG) to correct roles, and/or transactions SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the Authorization Info System (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SE16, TCD=SE16N, TCD=SE17, TCD=SM30, or TCD=SM31 [and all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT=03 DICBERCLASS=&NC&

### 6.1.1.7 External Clients Are Allowed to Switch the Profile Level (0702)

**Purpose**
To check whether external clients are allowed to switch the profile level for the Internet Communication Framework (ICF).

**Procedure**
The profile parameter icf/accept_remote_profile_level is checked. Return value is 0 (not allowed, default) or 1 (allowed).

**Risk Rating**
The rating is set automatically as follows:

GREEN: The parameter is set to 0 or does not exist.

RED: The parameter is set to 1.

RED:

**Evaluated Risk - High**
This trace allows denial of service attacks and might contain sensitive data. HTTP requests are also slower if this option is used.

Recommendation: Omit parameter icf/accept_remote_profile_level or set it to 0. This trace can be used for diagnostic purposes but should be activated (set to 1) only in exceptional cases and for a short time.

This setting creates vulnerability in terms of "denial of services" in your system.

### 6.1.1.7.1 External Clients Are Allowed to Switch the Profile Level (0702)

### 6.1.2 http Client

#### 6.1.2.1 Additional http Client Connections Found (0682)

**Purpose**
To avoid unauthorized communication to other SAP or non-SAP systems.

**Procedure**
Check the table RFCDES and search for entries with RFCTYPE = "H" or "G" which are not mentioned in the questionnaire.

**Risk Rating**
The rating is set automatically as follows:

GREEN: No additional HTTP client connection.
RED: At least one additional HTTP client connection.

RED:
Evaluated Risk - High
Recommendation: There is at least one additional HTTP client connection not specified in the questionnaire. We recommend that you check this connection.
Check the RFCDES table and search for entries with RFCTYPE = 'H' or 'G'.

6.1.2.2 No Proxy Used to Connect to http Servers (0683)
Purpose
To check whether all connections to an HTTP server use a proxy.

Procedure
Check whether the proxy is globally maintained in table PPROXY_G. If not, the use of the proxy has to be customized in table RFCDES.

Risk Rating
The rating is set automatically as follows:
GREEN: HTTP proxy configured.
YELLOW: No HTTP proxy configured for at least one connection.

YELLOW:
Evaluated Risk - Medium
Recommendation: We found at least one connection to an HTTP server that does not use a proxy. A proxy works as a security barrier between the internal network and the Internet and should always be used.
Check whether the proxy is globally maintained in table PPROXY_G. If not, use of the proxy must be customized in the RFCDES table.

6.1.2.3 No Authorization for S_SICF Required for http Client Access (0684)
Purpose
To check whether HTTP client access is protected by means of authorizations.

Procedure
Check the customizing in table RFCDES.

Risk Rating
The rating is set automatically as follows:
GREEN: No HTTP client connection without authorization.
YELLOW: At least one HTTP client connection without authorization.

YELLOW:
Evaluated Risk - Medium
Recommendation: We found at least one HTTP client connection that does not require authorization. You should request authentication for all HTTP clients.
Check the customizing in table RFCDES.

6.1.2.4 Client Proxy Does Not Require Client Authentication (0685)
Purpose
To check whether the client proxy demands client authorization.

Procedure
Check whether the proxy authorization is globally maintained in the tables PPROXY_G and PPROXY_C. If it is not, the use of the proxy has to be customized in table RFCDES.

Risk Rating
The rating is set automatically as follows:
GREEN: Proxy requires client authentication.
YELLOW: At least one connection without authentication configured in the client proxy.

YELLOW:
Evaluated Risk - Medium
Recommendation: We found at least one connection for which the client proxy does not require authentication. You should request authentication for all proxies. Check whether proxy authorization is globally maintained in the PPROXY_G and PPROXY_C tables. If this is not the case, use of the proxy must be customized in the RFCDES table.

6.1.2.5 Additional http Connections with Full Logon Data Found (0687)

Purpose
To check whether there are HTTP connections with full logon data that are not specified in the questionnaire.

Procedure
Check the HTTP connection settings in table RFCDES.

Risk Rating
The rating is set automatically as follows:
GREEN: No additional connections found with full logon data that were not specified in the questionnaire.
RED: Connections found with full logon data that were not specified in the questionnaire.

Evaluated Risk - High
Recommendation: We found HTTP connections with full logon data that were not specified in the questionnaire. We recommend you check these HTTP connections.

6.1.2.6 No Encryption of Outgoing http Communication (0688)

Purpose
To check the encryption of outgoing HTTP connections.

Procedure
Check the connection settings in table RFCDES.

Risk Rating
The rating is set automatically as follows:
GREEN: SSL secured communication is configured.
RED: At least one HTTP connection found without SSL encryption.

Evaluated Risk - High
Recommendation: We found at least one HTTP connection without SSL encryption. This can be dangerous, especially if a password is required for authentication, because the user and password are not transferred in encrypted format if SSL is not used. We recommend that you use SSL encryption for your HTTP connections.

Check the connection settings in the RFCDES table.

6.1.3 Internet Communication Manager (ICM)

6.1.3.1 Users - Other Than System Administrators - Are Authorized to Administrate the ICM (0701)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
GREEN: No users found (except specified in the questionnaire) with surplus authorizations.
YELLOW/RED: Additional users found with surplus authorizations. The rating depends on the severity of this check.
RED:

Evaluated Risk - High
GREEN:
**Evaluated Risk - None**
Unauthorized administration (such as start and stop) of Internet Communication Manager (ICM).
Recommendation: Use the Profile Generator (PFCG) to correct roles, and/or transactions SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the Authorization Info System (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SMICM [and all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD=PADM

6.1.3.2 Users - Other Than System Administrators - Are Authorized to Display the http Server Cache (0705)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
**GREEN:** No users found (except specified in the questionnaire) with surplus authorizations.
**YELLOW/RED:** Additional users found with surplus authorizations. The rating depends on the severity of this check.

**RED:**
**Evaluated Risk - High**
**GREEN:**
**Evaluated Risk - None**

Unauthorized access to sensitive data.
Recommendation: Use the Profile Generator (PFCG) to correct roles, and/or transactions SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the Authorization Info System (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD=SMICM [and all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD=PADM

6.1.3.3 Users - Other Than System Administrators - Are Authorized to Configure the ICM Monitor (0706)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):
**GREEN:** No users found (except specified in the questionnaire) with surplus authorizations.
**YELLOW/RED:** Additional users found with surplus authorizations. The rating depends on the severity of this check.

**RED:**
**Evaluated Risk - High**
**GREEN:**
**Evaluated Risk - None**

Unauthorized change of ICM services.
Recommendation: Use the Profile Generator (PFCG) to correct roles, and/or transactions SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the Authorization Info System (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD=SMICM [and all relevant parameter transactions]
Object 2: S_ADMI_FCD with S_ADMI_FCD=PADM

6.1.3.4 External Clients Are Allowed to Switch the Trace Level (0703)

Purpose
To check whether external clients are allowed to switch the trace level for the Internet Communication Manager (ICM).

Procedure
The profile parameter icm/accept_remote_trace_level is checked. Return value is 0 (not allowed, default) or 1 (allowed).

Risk Rating
The rating is set automatically as follows:
GREEN: The parameter is set to 0 or does not exist.
RED: The parameter is set to 1.

Evaluated Risk - High
This trace allows access to system data that could be misused for a subsequent attack.
Recommendation: Omit parameter icm/accept_remote_trace_level or set it to 0. This trace can be used for diagnostic purposes but should be activated (= set to 1) only in exceptional cases and for a short time.

6.1.3.4.1 External Clients Are Allowed to Switch the Trace Level (0703)

6.1.3.5 ICM (Internet Communication Manager) Is Active (0704)

Purpose
To check whether the Internet Communication Manager (ICM) has been started.

Procedure
The profile parameter rdisp/start_icman is checked. Return value is true (started, default) or false (not started).

Risk Rating
The rating is set automatically as follows:
Skip: The parameter is set to false.
Show: The parameter is set to true or does not exist.
YELLOW:
Recommendation: The Internet Communication Manager (ICM) is started on your system. Check whether the ICM is used in your environment. If it is not used, deactivate the ICM by setting the profile parameter rdisp/start_icman to false in order to reduce the risk.

6.1.3.5.1 ICM (Internet Communication Manager) Is Active (0704)

6.1.3.6 Not all http Service Requests Are Logged (0662)

Purpose
To check whether logging is enabled for all available HTTP services.

Procedure
Look for available HTTP services and check whether profile parameters icm/HTTP/logging_ = PREFIX=<URL Prefix> are set for all of them.
Use the report RSPFPAR to visualize the profile parameters.

Risk Rating
Set the rating manually as follows:

**GREEN:** Logging activated for URL prefix '/'.

**YELLOW:** Logging not activated or not activated for all available HTTP services.

**YELLOW:**

**Evaluated Risk - Medium**

Logging is not activated for some or all of the available HTTP services.

**Threat:** Lack of information to track security violations

**Recommendation:**

Enable logging for all available HTTP services by setting the profile parameters icm/HTTP/logging_ = PREFIX=<URL Prefix>. For more information, see the online documentation for these profile parameters.

### 6.1.4 PSE Management

#### 6.1.4.1 Users - Other Than System Administrators - Are Authorized to Maintain the System PSE's (0711)

**Purpose**

To find users with more authorizations than needed for their tasks.

**Procedure**

ST14 download data is analyzed and rated automatically, but individually for each check.

**Risk Rating**

The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

**GREEN:** No users found (except specified in the questionnaire) with surplus authorizations.

**YELLOW/RED:** Additional users found with surplus authorizations. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

**GREEN:**

**Evaluated Risk - None**

Unauthorized access to system certificates.

**Recommendation:** Use the Profile Generator (PFCG) to correct roles, and/or transactions SU02 (Maintain Profiles)/SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the Authorization Info System (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

**Authorization objects:**

Object 1: S_TCODE with TCD=STRUST [and all relevant parameter transactions]

Object 2: S_ADMI_FCD with S_ADMI_FCD=NADM

Object 3: S_RZLADM with ACTVT=01

Object 4: S_TABU_DIS with ACTVT=02 and DICBERCLS=SS

### 6.1.5 J2EE - Backend Checks (Dual Stack System)

#### 6.1.5.1 Users with Role "SAP_J2EE_ADMIN" (0813)

**Purpose**

To check if any users other than the system administrators have the role SAP_J2EE_ADMIN (Add-In installation) or the role defined during the installation (for example, J2EE_ADMIN_<SID>).

**Procedure**

List the users with this role in the check table.

**Rating**

Rating takes place automatically as follows:

**GREEN:** Only system administrators have the role.

**RED:** Other users have the role.
Purpose
To check if any users other than the system administrators have the role SAP_J2EE_ADMIN (Add-In installation) or the role defined during the installation (for example, J2EE_ADM_<SID>).

Procedure
List the users with this role in the check table.

Rating
Rating takes place automatically as follows:
GREEN: Only system administrators have the role.
RED: Other users have the role.

Evaluation Risk - High

Recommendation: The following users have either the role SAP_J2EE_ADMIN (Add-In installation) or J2EE_ADM_<SID>, which allows system administration. Please review these users and consider removing all users who do not need system administration rights.
Check whether user is assigned to the system Java Administrators group:
- AS Java only (with DB or LDAP as DataSource): List users (and groups) assigned to Java group "Administrators"
- Dual stack: List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"
- AS Java only (with ABAP as DataSource): List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"

Recommendation: The following users have either the role SAP_J2EE_ADMIN (Add-In installation) or J2EE_ADM_<SID>, which allows system administration. Please review these users and consider removing all users who do not need system administration rights.
Check whether user is assigned to the system Java Administrators group:
- AS Java only (with DB or LDAP as DataSource): List users (and groups) assigned to Java group "Administrators"
- Dual stack: List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"
- AS Java only (with ABAP as DataSource): List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"

6.1.5.2 Guest user should be locked (J135)

Purpose:
To check whether the guest user is locked.

Procedure:
Check whether the guest user is locked.

Rating:
Set the rating to GREEN if the guest user is locked.
Set the rating to RED if the guest user is not locked.

Background:
Lock the guest user.

Evaluation Risk - High

Recommendation: Lock the guest user.

6.1.5.3 Guest User should be locked (J136)

Purpose:

Procedure:

Rating:
Set the rating to GREEN if only well-known users have the EVERYONE role.
Set the rating to RED if there are unknown users with the EVERYONE role.
Background:
Remove the EVERYONE role for unknown users.

**RED:**

**Evaluated Risk - High**

**Recommendation:** Remove the EVERYONE role for unknown users.

6.1.5.4 Profile of User SAPJSF (0796)

**Purpose:**
To check whether the communication user SAPJSF has the appropriate rights only.

**Procedure:**
Automatic check:
The system checks whether the SAPJSF user has the profile SAP_ALL.

**Risk Rating:**
Rating takes place automatically as follows:
**GREEN:** User SAPJSF does not have the profile SAP_ALL or does not exist.
**RED:** User SAPJSF has the profile SAP_ALL.

**Purpose:**
To check whether the communication user SAPJSF has the appropriate rights only.

**Procedure:**
Automatic check:
The system checks whether the SAPJSF user has the profile SAP_ALL.

**Risk Rating:**
Rating takes place automatically as follows:
**GREEN:** User SAPJSF does not have the profile SAP_ALL or does not exist.
**RED:** User SAPJSF has the profile SAP_ALL.

**Evaluated Risk - High**

**Recommendation:** The SAPJSF user should only have the role SAP_BC_JSF_COMMUNICATION and not SAP_ALL. You should also rename this user. To rename this user, change the "ume.r3.connection.master.user" in the sapum.properties file (or in the file that you specified as ume.cfg.file.).

6.1.5.5 Type of Users in the Jco RFC Provider (0877)

**Purpose:**
To check whether the users specified in the JCo RFC Provider are of type "Communication"; only "UMEBackendConnection" connection should be available.

**Procedure:**

**Command Line:** IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 730
1. Log on to the Visual Administrator as administrator.
2. On the left side of the screen, expand Cluster -> Server -> Services.
3. Select the JCo RFC Provider from the list of services.
4. Check the available RFC destinations pointing at the ABAP stack of your system on the "Runtime" tab page.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).

**Command Line:** ELSEIF "YSAP-SERVERCORE" >= 730 AND "YSAP-SERVERCORE" <= 740
1. Log on to the NWA as administrator.
3. Filter for RFC destination.
4. For each destination found, check the user in the "Logon Data" tab destination detail.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).

Command Line: ENDIF

Risk Rating:
Set the rating manually as follows:
GREEN: Only "UMEBackendConnection2 and well-known connections are available.
RED: Unknown connections are available.

Purpose:
To check whether the users specified in the JCo RFC Provider are of type "Communication"; only "UMEBackendConnection" connection should be available.

Procedure:

Command Line: IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 730
1. Log on to the Visual Administrator as administrator.
2. On the left side of the screen, expand Cluster -> Server -> Services.
3. Select the JCo RFC Provider from the list of services.
4. Check the available RFC destinations pointing at the ABAP stack of your system on the "Runtime" tab page.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).

Command Line: ELSEIF "YSAP-SERVERCORE" >= 730 AND "YSAP-SERVERCORE" <= 740
1. Log on to the NWA as administrator.
3. Filter for RFC destination.
4. For each destination found, check the user in the "Logon Data" tab destination detail.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).

Command Line: ENDIF

Risk Rating:
Set the rating manually as follows:
GREEN: Only "UMEBackendConnection2 and well-known connections are available.
RED: Unknown connections are available.

RED:

Evaluated Risk - High

Recommendation: Use only users of type "Communication" for your JCo RFC connections to prevent dialog logon with communication users. There is at least one RFC connection with a user of another user type in your system.

Recommendation: Use only users of type "Communication" for your JCo RFC connections to prevent dialog logon with communication users. There is at least one RFC connection with a user of another user type in your system.

6.1.5.6 Authorization of Users in the Jco RFC Provider (0878)

Purpose:
To check whether the users specified in the JCo RFC Provider have surplus authorizations.

Procedure:

Command Line: IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 720
1. Log on to the Visual Administrator as administrator.
2. On the left side of the screen, expand Cluster -> Server -> Services.
3. Select the JCo RFC Provider from the list of services.
4. Check the available RFC destinations on the "Runtime" tab page.
5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).
**SC_WEBAS - Web Application Server**

**Command Line**: ELSEIF "YSAP-SERVERCORE" >= 720 AND "YSAP-SERVERCORE" <= 740
1. Log on to the NWA as administrator.
3. Filter for RFC destination.
4. For each destination found, check the user in the "Logon Data" tab destination detail.
5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

**Command Line**: ENDIF

**Risk Rating**:
Set the rating manually as follows:
- **GREEN**: Users in JCo RFC Provider are well-known.
- **RED**: Users in JCo RFC Provider are not well-known.

**Purpose**:
To check whether the users specified in the JCo RFC Provider have surplus authorizations.

**Procedure**:

**Command Line**: IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 720
1. Log on to the Visual Administrator as administrator.
2. On the left side of the screen, expand Cluster -> Server -> Services.
3. Select the JCo RFC Provider from the list of services.
4. Check the available RFC destinations on the "Runtime" tab page.
5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

**Command Line**: ELSEIF "YSAP-SERVERCORE" >= 720 AND "YSAP-SERVERCORE" <= 740
1. Log on to the NWA as administrator.
3. Filter for RFC destination.
4. For each destination found, check the user in the "Logon Data" tab destination detail.
5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

**Command Line**: ENDIF

**Risk Rating**:
Set the rating manually as follows:
- **GREEN**: Users in JCo RFC Provider are well-known.
- **RED**: Users in JCo RFC Provider are not well-known.

**Evaluated Risk - High RED:**

**Recommendation**: Do not give too many authorizations to the users used for JCo RFC connections. There is at least one RFC user with the profile SAP_ALL in your system or a user with more than 80% of all authorizations.

**Recommendation**: Do not give too many authorizations to the users used for JCo RFC connections. There is at least one RFC user with the profile SAP_ALL in your system or a user with more than 80% of all authorizations.

**6.1.5.7 J2EE Engines Allowed to Access the Application Server (0881)**

**Purpose**
To check which J2EE Engines are allowed to access the application server.

**Procedure**
Automatic check:
The J2EE Engines in table SNCSYSACL are listed.

**Risk Rating**
No rating for this check. The J2EE Engines are listed.
Purpose
To check which J2EE Engines are allowed to access the application server.

Procedure
Automatic check:
The J2EE Engines in table SNCSYSACL are listed.

Risk Rating
No rating for this check. The J2EE Engines are listed.

YELLOW:
Recommendation: These J2EE Engines are allowed to access the application server. Check the list. YELLOW:
Recommendation: These J2EE Engines are allowed to access the application server. Check the list.

6.1.5.8 Other J2EE Systems Allowed to Connect to the SAP Database for User Replication (0863)

Purpose:
To check for J2EE systems that are allowed to connect to the SAP database of the back-end system. The UME replication functionality still exists in newer releases, but is no longer documented since it is obsolete as of NW 7.00.

Procedure:
List the systems specified in SMUM_ACL of the back-end system. Check whether all of these systems exist in the property file ume.r3.sync.sender in the Visual Administrator.

Risk Rating:
No rating for this check. Include the following information in the report: 1) If more systems appear in the table than in ume.r3.sync.sender, indicate any additional systems. 2) If user replication is not used but entries exist in the table SMUM_ACL, indicate the entries as displayed in the table SMUM_ACL. To include this information in the report, choose "Show".

Purpose:
To check for J2EE systems that are allowed to connect to the SAP database of the back-end system. The UME replication functionality still exists in newer releases, but is no longer documented since it is obsolete as of NW 7.00.

Procedure:
List the systems specified in SMUM_ACL of the back-end system. Check whether all of these systems exist in the property file ume.r3.sync.sender in the Visual Administrator.

Risk Rating:
No rating for this check. Include the following information in the report: 1) If more systems appear in the table than in ume.r3.sync.sender, indicate any additional systems. 2) If user replication is not used but entries exist in the table SMUM_ACL, indicate the entries as displayed in the table SMUM_ACL. To include this information in the report, choose "Show".

YELLOW:
Recommendation: We found values in the SMUM_ACL file in your back-end system that do not exist in the property file ume.r3.sync.sender. Check your configuration. If you do use user replication, this file should be empty. YELLOW:
Recommendation: We found values in the SMUM_ACL file in your back-end system that do not exist in the property file ume.r3.sync.sender. Check your configuration. If you do use user replication, this file should be empty.

6.1.5.9 Users Authorized to Maintain the Sending Systems for User Replication (0864)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data is analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible
values (Green / Yellow / Red):
Green: No users found (except specified in the questionnaire) with exceeding authorizations.
Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data is analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

Green: No users found (except specified in the questionnaire) with exceeding authorizations.
Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High

Evaluated Risk - High

This authorization allows a user to maintain the access control list for sending systems. Currently, it is possible to create users from a malicious external system.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check, you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD = SE16, SE17, SM30, or SM31 [and all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT = 2 and DICBERCLS = SUSR

This authorization allows a user to maintain the access control list for sending systems. Currently, it is possible to create users from a malicious external system.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check, you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TCODE with TCD = SE16, SE17, SM30, or SM31 [and all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT = 2 and DICBERCLS = SUSR
7 SC_HR - SC Human Resources Modul

7.1 Human Resources

7.1.1 Human Resources General Checks

7.1.1.1 Users - Other Than HR Administrators - Are Authorized to Maintain Table T77S0 (0922)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

Green: No users found (except specified in the questionnaire) with exceeding authorizations.

Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
Users having this authorization can change or deactivate the use of the authorization objects P_PERNR and P_ORGIN in the HR application.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TABU_DIS with DICBERCLS = PS and ACTVT = 02
Object 2: S_TCODE with TCD = SE16, SE16N, SE17, SM30, or SM31 [and all relevant parameter transactions]

7.1.1.2 Users - Other Than HR Administrators - Are Authorized to Maintain Tables for Organizational Data (0923)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

Green: No users found (except specified in the questionnaire) with exceeding authorizations.

Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
Users having this authorization can change the logging of infotypes and report starts. Also organizational HR data tables such as T500P T501 or T503K can be changed.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM)
you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TABU_DIS with DICBERCLS = PC and ACTVT = 02
Object 2: S_TCODE with TCD = SE16, SE16N, SE17, SM30, or SM31 [including all relevant parameter transactions]

7.1.1.3 Users - Other Than HR Administrators - Are Authorized to Read the Infotype Change Log (0924)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):
Green: No users found (except specified in the questionnaire) with exceeding authorizations.
Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
Users having this authorization can access infotype data without a specific authorization for infotypes.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_PROGRAM with P_GROUP = RPUAUD00 and P_ACTION = SUBMIT
Object 2: S_TCODE with TCD = SE38 or SA38 or SC38 (and all relevant parameter transactions)
Object 3: S_DEVELOP ACTVT = 03

7.1.1.4 Users - Other Than HR Administrators - Are Authorized to Read HR Tables with Person Related Data (0925)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):
Green: No users found (except specified in the questionnaire) with exceeding authorizations.
Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
Users with this authorization can read all HR tables with person-related data.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TABU_Dis = PA and ACTVT = 03
Object 2: S_TCODE = SE16, SE16N, SE17, SM30, or SM31 [and all relevant parameter transactions]

7.1.1.5 Users - Other Than HR Administrators - Are Authorized to Change HR Tables with Person Related Data (0926)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):
- **Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - High**
Users with this authorization can change all HR tables with person-related data.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions
SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TABU_Dis = PA and ACTVT = 02
Object 2: S_TCODE = SE16, SE16N, SE17, SM30, or SM31 [including all relevant parameter transactions]

7.1.1.6 Users - Other Than HR Administrators - Are Authorized to Maintain Client Dependant HR Customizing (0927)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):
- **Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**Evaluated Risk - High**
Users with this authorization can change client-dependant HR customizing.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions
SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: S_TABU_Dis = PA AND PS and ACTVT = 02
Object 2: S_TCODE = SE16, SE16N, SE17, SM30, or SM31 [and all relevant parameter transactions]
7.1.1.7 Users - Other Than HR Administrators - Are Authorized to Run All HR Transactions (0928)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

- **Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

*Evaluated Risk - High*

Users with this authorization can call all HR transactions.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object1: S_TCODE = P*
- Object2: P_TCODE = *

7.1.1.8 Users - Other Than HR Administrators - Have Broad Authorization on HR Reports (0929)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

- **Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

*Evaluated Risk - High*

This authorization gives broad authorization for HR Reports. The authorization objects P_ORGIN and P_PERNR can be overruled with this authorization.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object1: P_ABAP = with REPID = * and COARS = 2

7.1.2 Personal Administration

7.1.2.1 Users - Other Than HR Administrators - Are Authorized to Read HR Master Data (0936)

Purpose
To find users with more authorizations than needed for their tasks.
**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

- **Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
Users with this authorization can read the HR master data.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE = PA20 [and all relevant parameter transactions]
- Object 2: P_ORGIN with AUTHC = R
- Object 3: P_ORGXX with AUTHC = R (if AUTHSW ORGXX is set to 1 in table T77S0)

**7.1.2.2 Users - Other Than HR Administrators - Are Authorized to Change Master Data without Double Verification (0937)**

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

- **Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**
Users with this authorization can change master data without verification through a colleague.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE = PA30 [and all relevant parameter transactions]
- Object 2: P_ORGIN with AUTHC = (D and ( E or S )) OR W
- Object 3: P_ORGXX with AUTHC = R (if AUTHSW ORGXX = 1 in table T77S0)

**7.1.2.3 Users - Other Than HR Administrators - Are Authorized to Delete Personnel Numbers (0938)**

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):
**Green**: No users found (except specified in the questionnaire) with exceeding authorizations. **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

Users with this authorization can delete personnel numbers. Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE = SE38 SA38 SC38 [as well as all relevant parameter transactions]
- Object 2: S_PROGRAM with P_GROUP = RPUDELPN and P_ACTION = SUBMIT
- Object 3: S_DEVELOP with ACTVT = 03
- OR
- Object 1: S_TCODE = PU00 [as well as all relevant parameter transactions]
- Object 2: P_TCODE = PU00
- Object 3: P_ORGIN with AUTHC = W

7.1.2.4 Users - Other Than HR Administrators - Are Authorized to Change their Own Master Data (0939)

**Purpose**

To find users with more authorizations than needed for their tasks.

**Procedure**

ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**

The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

**Green**: No users found (except specified in the questionnaire) with exceeding authorizations. **Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

Users with this authorization can change their own personnel data. Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- Object 1: S_TCODE = PA30 [and all relevant parameter transactions]
- Object 2: P_PERNR with P_SIGN = "I"

7.1.3 Payroll

7.1.3.1 Users - Other Than HR Administrators - Are Authorized to Read Payroll Results (0946)

**Purpose**

To find users with more authorizations than needed for their tasks.

**Procedure**

ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**

The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):
**Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
**Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

Users with this authorization can read the HR payroll results.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUI) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
Object 1: P_PCLX = with AUTHC = 'R' and RELID = ''

7.1.3.2 Users - Other Than HR Administrators - Are Authorized to Maintain Personell Calculation Schemas (0947)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

**Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
**Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

Users having this authorization can maintain the HR personnel calculation schemas.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUI) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: P_TCODE with TCD = PE01
Object 2: S_TCODE with TCD = PE01 [and all relevant parameter transactions]

7.1.3.3 Users - Other Than HR Administrators - Are Authorized to Release a Payroll Run (0950)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data are analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

**Green**: No users found (except specified in the questionnaire) with exceeding authorizations.
**Yellow/Red**: More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

**Evaluated Risk - High**

Users with this authorization can release a payroll run.
Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and
authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: P_TCODE with TCD = PA03
Object 2: S_TCODE with TCD = PA03 [and all relevant parameter transactions]

7.1.3.4 Users - Other Than HR Administrators - Are Authorized to Delete Payroll Results (0951)

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data are analyzed and rated automatically but individually for each check.

Risk Rating
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

Green : No users found (except specified in the questionnaire) with exceeding authorizations.
Yellow/Red: More users with exceeding authorizations were found. The rating depends on the severity of this check.

RED:

Evaluated Risk - High
Users with this authorization can delete payroll results.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check you should inspect the roles or profiles that include the authorization objects listed below.

Authorization Objects:
Object 1: S_TCODE = SE38 SA38 SC38 [and all relevant parameter transactions]
Object 2: S_PROGRAM with P_GROUP = RPUDEL20 and P_ACTION = SUBMIT
Object 3: S_DEVELOP with ACTVT = 03
OR
Object 1: S_TCODE = PU01 and P_TCODE = PU01 [and all relevant parameter transactions]
Object 2: P_ORGIN with AUTHC = W
8 SC_CustomerChecks - Group for Customer Specific Checks

8.1 Customer Specific Authorization Checks

The following checks display the users found in the customer-defined key figures between 9000 and 9999. If no customer checks are defined, this check is rated GREEN, and no subchecks are created. The authorization combinations for these checks are defined in transaction ST13 (tool: SOS_CUSTOMER_DATA).

The users have the authorization that you defined in the analyzed system, under the corresponding key figure, using transaction ST13 and selecting the SOS_CUSTOMER_DATA tool.

Key figure 9000 is an example shipped with the system, that lists all users who have authorization to delete table change logs.

If you do not want to perform this check, delete the example (key figure 9000), using transaction ST13 (selecting tool SOS_CUSTOMER_DATA) in the system to be analyzed. You can see other samples by ticking the box 'Also Show SAP Entries:' in the tool SOS_CUSTOMER_DATA.

8.1.1 <;GENERAL;KeyfigName>

Purpose
To find users with more authorizations than needed for their tasks.

Procedure
ST14 download data is analyzed and rated automatically, but individually for each check.

Risk Rating
The rating is set automatically as follows, but does not always include all three possible values (GREEN/YELLOW/RED):

GREEN: No users found (except those specified in the questionnaire) with surplus authorizations.

YELLOW/RED: Users with surplus authorizations were found. The rating depends on the severity of this check.

RED:
Evaluated Risk - High
YELLOW:
Evaluated Risk - Medium

Recommendation: Depending on your environment, use the Profile Generator (PFCG) to correct roles, and transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations. You can check the results with the authorization info system (SUIM). For this check, inspect the roles or profiles that include the authorization objects found in the /SSA/ABS report.

8.2 Customer Defined Authorization Checks

Purpose
The following checks display the users found in the customer-defined authorization checks with key figure IDs between 9000 and 9999. These figures were defined in the questionnaire.

Procedure
The check is performed automatically.
SC_CUSTOMERCHECKS - Group for Customer Specific Checks

Rating
GREEN, if no users have been found that must not have the authorization
YELLOW, if users have been found that have the selected authorization and the criticality
was restricted to Medium in the questionnaire.
RED, if users have been found and the criticality was not restricted.
'Failure: Missmatch in Definition', if any of the sub checks shows a failure.
'Failure: Environment Issue', if the authorization check was defined in the questionnaire but
could not be processed on the managed system (see SAP Note 1608969)
If no customer defined authorization checks have been defined the check remains unrated
and the chapter is not shown in the service report.

Command Line: CASE "YSAP-SC_CUSTOMERCHECKS_RATING_OF_ROOT"

Command Line: WHEN '5'

Failure: Environment Issue - Analysis could not be not performed
The definition of the Customer Defined Authorization Checks was done in the Questionnaire.
However the required data collection could not be done on the managed system because the
mandatory prerequisites on the managed system have not been fulfilled. For details about the
prerequisites and how to fulfill they see SAP Note 1608969.

Command Line: WHEN OTHERS

Comment Line: OTHERS = 1 or 2 or 3 or 4  "Comment Line"
The following table provides an overview about authorization checks that were defined in the
SAP customer environment using the Questionnaire of the Security Optimization Service.

Command Line: ENDCASE

Command Line: CASE "YSAP-SC_CUSTOMERCHECKS_RATING_OF_ROOT"

Command Line: WHEN '1'

Command Line: WHEN '5'

Command Line: WHEN OTHERS

Comment Line: OTHERS = 2 or 3 or 4  "Comment Line"
Subchapters provide information for key figures that have been processed but show
deviations.
In detail you will find a table 'Users' list of example users per client as well as the count of
users with the analyzed authorizations. This list and counts exclude users (a) that have the
authorization profile SAP_ALL, (b) that are listed in the questionnaire as to be allowed for ALL
customer defined authorization checks and (c) that are listed in the questionnaire as to be
allowed for the individual key figure.
A risk level and an optional brief description are added according to your entries in the
questionnaire.
If the check was defined in the questionnaire the table 'Authorization Check' provides
technical information on the check definition. Authorizations for transactions (S_TCODE) are
combined with an 'or' while all other authorization objects are combined with 'and'.

Command Line: ENDCASE

8.2.1 <;GENERAL;KeyfigName>

Purpose
Provide information about the findings for an individual key figure.

Procedure
This check is performed automatically:
Tab Users provides information about the found users that are not allowed to have the
checked authorization. This list excludes users that (a) have the profile SAP_ALL, (b) have
been authorized using the questionnaire either for all customer defined authorization checks
or (c) for this individual key figure.
Tab Authorization Check provides a copy of the executed authorization check, if the check
was defined using the questionnaire. Authorizations for transaction codes (Object S_TCODE)
are linked with 'or' while all other authorization objects are linked with 'and'.
Tab Customer Defined Description provides a copy of the check description, if it was defined in the questionnaire.

**Rating**
GREEN, if no users with the critical authorization have been found.
YELLOW, if users with the critical authorizations were found and the criticality was set to Medium in the questionnaire.
RED, if users with the critical authorization were found.
FAILURE, if inconsistencies have been detected for the check (e.g. if check definition was changed between scheduling the data collection and executing the analysis session.
The check remains without a rating, if a key figure ID was declared in the questionnaire but the authorization to be checked was not specified in detail in the questionnaire.

**Evaluated Risk - Medium**
**Evaluated Risk - High**

**Mismatch in the Key Figure Definition:**
The analysis of this key figure could not be executed because the definition of the key figure was changed between the scheduling of the data collection and the evaluation in the analysis session.
9 SC_SAPROUTER - Checks for the SAProuter

9.1 SAProuter

Purpose
This check contains all SAProuter-relevant checks as child checks. When all child checks have been performed, this check must be rated accordingly.

Procedure
As the SAProuter checks are all designed manually, and the data that is to be checked is mainly located in the file SAPROUTTAB at the customer site, this file must either be transmitted to SAP or be available for viewing at the customer site.

An example of a SAPROUTTAB file is available in textual form for this check. The customer files, however, are different and are often not well documented; sometimes they contain just one or two lines with a lot of asterisks. This means that almost anything is permitted. This is a very simple way of setting up the SAPROUTTAB and is acceptable in an emergency situation, but must be changed immediately after the problem has been solved.

In most cases, however, the setting has not been changed, which results in a lot of checks with high vulnerability.

For detailed information about the SAProuter, see SAP Note 30289, and SAP Help Portal at http://help.sap.com. Use the "Search" function to search for "saprouter". Then look at the SAProuter functions so that you are familiar with this product.

(In particular, we recommend that you look at: Using SAProuter -> Route Permission Table.)

IP addresses of SAP servers:
- 194.117.106.129  sapserv1  (Walldorf, VPN)
- 194.39.131.34   sapserv2  (Walldorf, SNC)
- 147.204.2.5     sapserv3  (Walldorf)
- 204.79.199.2    sapserv4  (Foster City)
- 194.39.138.2    sapserv5  (Tokyo)
- 194.39.139.16   sapserv6  (Sydney)
- 194.39.134.35   sapserv7  (Singapore)

(This information is required for additional checks to determine which partners are allowed to communicate with the customer by means of the SAPROUTTAB.)

Risk Rating
The risk rating is performed automatically as part of the checks below, but is not currently reported.

Here, we check the configuration of your SAProuter.
The following is an example of a SAPROUTTAB with or without SNC:

**SAPROUTTAB with SNC:**
- SNC is used for communication with sapserv2 due to the existence of the following line for each protocol:
  KT "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 194.39.131.34 *
  - Access from all locations in the customer network to the
  - SAPNet - R/3 front end (SAP Support System) by means of sapserv2
  KP * "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 3299
  - SNC connection from SAP to the customer system for support
  - (One line of these for each system or application server)
  - Connection to the system PRD CI
  KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 10.3.4.20 3200 secret
  - Connection to system PRD special batch instance
  KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 10.3.4.20 3201 secret
SC_SAPROUTER - Checks for the SAProuter

- Connection to system PRD APPL1
  KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 10.3.4.21 3200 secret
- Connection to system PRD APPL2
  KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 10.3.4.22 3200 secret

- SNC connection from SAP to the customer system for Telnet
- Set up this connection ONLY if it is needed
- Telnet logon to PRD CI - temporary only
  KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 10.3.4.20 23 vsec

- Deny all other connections
  SAPROUTTAB without SNC:
  - Access from all locations in the customer network to the
  - SAPNet - R/3 front end (SAP Support System) by means of sapserv2
    P * 147.204.2.5 3299

- Connection from SAP to the customer system for support
- (One line of these for each system or application server)
- Connection to system PRD CI
  P 147.204.2.5 10.3.4.20 3200 secret
- Connection to system PRD special batch instance
  P 147.204.2.5 10.3.4.20 3201 secret
- Connection to system PRD APPL1
  P 147.204.2.5 10.3.4.21 3200 secret
- Connection to system PRD APPL2
  P 147.204.2.5 10.3.4.22 3200 secret

- SNC connection from SAP to the customer system for Telnet
- Set up this connection ONLY if it is needed
- Telnet logon to PRD CI - temporary only
  P 147.204.2.5 10.3.4.20 23 vsec

- Deny all other connections
  D * * *

9.1.1 No Encryption (SNC or VPN) Used for the Connection to SAP (0541)

Purpose
To check whether customers are still using the "old" communication mode (without SNC encryption) or whether they have already changed to the new options with more security and less costs.

Procedure
Use transaction STFK in system CSx to check the SAProuter information for the customer. Navigate to the service connection for the system that you are looking for. Choose Edit -> Status (Shift-F4) to find out which sapserv is used. (This only works if at least one connection to the customer is open.) sapserv3 and higher support encryption if encryption is activated in the SAPROUTTAB at the customer site, but they are not available on the Internet. This means that the line from SAP to the customer (and the other way around) always has to be paid by the customer. sapserv1(a) always uses VPN and is located on the Internet. sapserv2(a) always uses SNC and is also located on the Internet.

To determine whether SNC is in use with sapserv3 and higher, you have to search for a "KT" entry in the SAPROUTTAB that is similar to the following entry:
KT "p:CN=sapserv3, OU=SAProuter, O=SAP, C=DE" 147.204.2.5 *

Rating
Set the rating manually as follows:
SNC GREEN sapserv2: sapserv2 is used.
SNC GREEN sapserv3 and higher: sapserv3 or higher, but the KT entry exists.
VPN GREEN sapserv1: sapserv1 is used.
No Encryption: Encryption is not used.

YELLOW:
Evaluated Risk - MEDIUM
Encryption is not used for the SAProuter connection to SAP. Without encryption, communication could be intercepted.
Recommendation: Read the instructions for creating an SAProuter SNC connection to SAP (see SAP Service Marketplace at service.sap.com/saprouter-sncdoc). If you want to use a VPN connection instead, see service.sap.com/access-support -> Remote Connectivity -> Internet Connections -> VPN Fundamentals.
If your SAProuter runs on iSeries, see SAP Note 567853.
By using sapserv1, SAP supports VPN, and by using sapserv2, it supports SNC encryption by means of the Internet. By using sapserv3 and higher, SAP also supports the use of SNC. However, as this server is not located on the Internet, you still need your private line to SAP, which could be dropped and replaced with the Internet connection if you use sapserv2 with SNC, or sapserv1 with VPN to SAP. All these encryption techniques ensure that your communication remains private. sapserv1 and sapserv2 also reduce costs at the customer site if a permanent Internet connection with a fixed IP address has to be available.

9.1.2 Non SNC-protected Communication from the Internet Allowed in the Saprountab (0542)

Purpose
In the SNC scenario, the SAProuter runs directly on the Internet. This means that you have to make sure that only SAP can connect to the router and that no other partners can (especially those who do not use encryption).

Procedure
A connection is set to SNC by means of the entry KT for this connection. This is the case for the connection to SAP. No other connection is allowed from the Internet by means of P or S (except for the service 3299 on sapservX, which is often used for the local users who routed to SAP).

Rating
Set the rating manually as follows:
GREEN: sapserv1 or sapserv3-7 is used or only SNC is permitted on the Internet when sapserv2 is used.
RED: Communication without SNC on the Internet by means of sapserv2 is also permitted (except for the service 3299 on sapservX, which is often used for the local users who routed to SAP).

Evaluated Risk - HIGH
You currently allow communication without SNC on the Internet. This is very risky because communication could be intercepted and misused by third parties.
Since you want to support SNC communication by means of this link only, use only KP or KS and no P in your SAPROUTTAB. The following is an example of how not to configure the SAPROUTTAB:

KT "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 194.39.131.34 *
KP "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 10.1.2.3 3254
P * * *

Here, the "P * * " entry allows communication without encryption on the Internet with any other partner.
Recommendation: Change the configuration as follows:
SC_SAPROUTER - Checks for the SAProuter

KT "p:CN=sapserv2, OU=SAProuter, O=SAP, C=DE" 194.39.131.34 *
KP * * *
P * * 3299

This at least ensures that only encrypted communication with trusted partners can be set up. Do not use the entry "KP * * *" because you must always avoid the "*" character. However, as this is restricted to SNC communication it is normally ensured that you can communicate with SAP only, because you normally have only one KT entry in your SAPROUTTAB.

Implementation: After you have found out which communication takes place by means of the SAProuter, you can update the SAPROUTTAB and either restart the SAProuter, or use option "-n" to activate the new SAPROUTTAB without canceling all the active connections.

This SAProuter runs on the Internet by means of SNC. It is therefore necessary that all communication takes place by means of SNC; otherwise intruders might be able to use the SAProuter to access your systems.

9.1.3 SAProuter Allows General Access to All Customers SAP Systems from Everywhere (0543)

Purpose
To check for "P * * *" (and similar entries), which indicate that somebody wanted to have the SAProuter running without thinking about which connections are needed. This check finds this entry and alerts the customer.

Procedure
Is the entry "P * * *", "P * * <SAProuter Pwd>", "S * * *", or "S * * <SAProuter Pwd>" used in the SAPROUTTAB?

Rating
Set the rating manually as follows:
GREEN: These entries are not in use.
YELLOW: All of these entries are secured by SAProuter passwords.
RED: At least one of these entries is in use without a SAProuter password.

RED: Evaluated Risk - HIGH
Any external party can go to anywhere internally, and the other way round, for all "SAP communication" (mostly by means of the destination services 32xx).
This is permitted without SAProuter passwords.
Recommendation: Only the required destination services and hosts must be mentioned explicitly in the SAPROUTTAB to have an overview of what is happening.

YELLOW: Evaluated Risk - MEDIUM
All external parties can access all of your internal systems, and the other way round, for your entire "SAP communication" (mostly by means of the destination services 32xx).
Fortunately, SAProuter passwords are in use here.
Recommendation: Only name the required destination services and hosts in the SAPROUTTAB so that you have an overview of access to your systems.
The SAProuter causes a "large hole" in a customer firewall, because all traffic that is routed by the SAProuter is encapsulated in TCP/IP packets that are routed by means of one specific service (mostly 3299). This means that a customer firewall cannot distinguish between different destination services, but just between the source and destination hosts.

9.1.4 SAProuter Allows Generic Communication Partners (Incoming) *(0544)*

Purpose
To check whether different (generic) communication partners have access to the customer’s network by means of the SAProuter. This is the case for very few destinations only. This means that especially in the source destination, there should not be an asterisk. This would make it possible for other unwanted attackers to gain access as well.
Procedure
Is the source host fully qualified or does it contain an asterisk? (Except for service 3299, which the SAProuter runs on and which is used for the local users to route to SAP.)

Rating
Set the rating manually as follows:
GREEN: No entries contain an asterisk as the source host except for port 3299.
YELLOW: An asterisk is part of the source host only (147.204.2.*, for example).
RED: There are entries that contain an asterisk in the source host.

RED:
Evaluated Risk - HIGH
There are entries in your SAPROUTTAB that contain an asterisk in the source host. If the source host is not fully qualified, intruders could use this route to access the system. (Except for the service 3299 on sapservX, which is often used for local users who are routed to SAP.) Recommendation: Find out how your SAProuter is used, which communication partners are used, and then set up a specially customized SAPROUTTAB.
Implementation: After you have found out what communication really takes place by means of the SAProuter, you can update the SAPROUTTAB, and either restart the SAProuter, or use option "-n" to activate the new SAPROUTTAB without canceling all the active connections.

YELLOW:
Evaluated Risk - MEDIUM
Some entries contain an asterisk as part of the source host (147.204.*, for example). If the source host is not fully qualified, intruders could use this route to access the system. (Except for the service 3299 on sapservX, which is often used for local users who are routed to SAP.) Recommendation: Find out how your SAProuter is used, which communication partners are used, and then set up a specially customized SAPROUTTAB.
Implementation: After you have found out what communication really takes place by means of the SAProuter, you can update the SAPROUTTAB, and either restart the SAProuter, or use option "-n" to activate the new SAPROUTTAB without canceling all the active connections.
To have a good overview of activity on the SAProuter, you have to remove wildcards such as "***" in the source hosts.

9.1.5 SAProuter Allows Generic Access to the Customers Servers (0545)

Purpose
The "destination host" determines the type of access to the customer's network. If you find generic access here, this means that the communication partners can route to any of the servers (and even clients) of the customer's system, because the SAProuter is running on or behind the customer's firewall.

Procedure
Is the destination host fully qualified or does it contain an asterisk? (Except for the port 3299)

Rating
Set the rating manually as follows:
GREEN: No entries contain asterisks for the destination host or asterisks exist only as part of the destination host (10.1.3.*, for example).
RED: There are asterisks in the destination host.

RED:
Evaluated Risk - HIGH
The destination host contains asterisks. This means that a particular source host can access many destination hosts at the customer site without further checks.
Your current SAPROUTTAB is similar to the following example:
P 147.204.2.5 * *
**SC_SAPROUTER - Checks for the SAProuter**

**Recommendation:** Find out which types of communication are used for which servers. The result may be similar to the following:

- SAP access to the PRD system
  P 147.204.2.5 10.3.2.1 3200
- SAP access to the PRU system
  P 147.204.2.5 10.3.2.1 3201
- SAP access to the QAS system
  P 147.204.2.5 10.3.2.5 3210
- SAP access to the DEV system
  P 147.204.2.5 10.3.2.11 3215

**Implementation:** once you have found out which type of communication is used by means of the SAProuter, you can update the SAPROUTTAB and either restart the SAProuter, or use the "-n" option to activate the new SAPROUTTAB without canceling all the active connections. To have a good overview of activity on the SAProuter, you have to remove wildcards such as "**" in the destination hosts, otherwise your entire network could be accessible by means of the SAProuter.

**9.1.6 Destination Service for SAProuter is Not Fully Qualified and Contains the Asterix (0546)**

**Purpose**
To check for an asterisk in the destination service, which means that for all ports with "SAP communication" (mostly 32xx), unrestricted access is permitted. This makes it easier to configure, but not to save. We recommend that you open only the required destination services so that you have an overview of the permitted access.

**Procedure**
Is the asterisk used in the SAPROUTTAB for the destination service?

**Rating**
Set rating is manually as follows:
GREEN: The destination service is always fully qualified.
YELLOW: In some cases, the destination service contains an asterisk.

**YELLOW:**

**Evaluated Risk - MEDIUM**
In some cases, the destination service contains an asterisk.
Access to all SAP systems is permitted (only by means of SAP communication, mostly on destination services 32xx).
This technique involves risks since nobody knows which service is actually in use. The following is an example of how your current SAPROUTTAB is configured:

P 147.204.2.5 10.3.2.1 *
P 147.204.2.5 10.3.2.5 *
P 147.204.2.5 10.3.2.11 *

**Recommendation:** Find out what communication is used for which servers. A possible result could be as follows:

- SAP access to the PRD system
  P 147.204.2.5 10.3.2.1 3200
- SAP access to the PRU system
  P 147.204.2.5 10.3.2.1 3201
- SAP access to the QAS system
  P 147.204.2.5 10.3.2.5 3210
- SAP access to the DEV system
  P 147.204.2.5 10.3.2.11 3215

**Implementation:** Once you have established what communication actually takes place by means of the SAProuter, you can update the SAPROUTTAB and either restart the SAProuter, or use the "-n" option to activate the new SAPROUTTAB without canceling all the active connections.
SC_SAPROUTER - Checks for the SAProuter

To have a good overview of activity on the SAProuter, you have to remove wildcards such as *** in the destination service.

9.1.7 SAProuter Allows Permanent OS Access (0548)

Purpose
To check that permanent direct OS access (service 23, 1503, or 5601) in the SAPROUTTAB is not granted as a general setting, as this is critical from a security point of view. This setting should only be activated at the request of the SAP Support Team, and should be deactivated immediately after the problem has been solved. At least a SAProuter password should be set and the source IP address restricted to SAP.

Procedure
Is permanent, direct OS access permitted in the SAPROUTTAB?

Risk Rating
Set the rating manually as follows:
GREEN: No direct OS access is permanently permitted.
YELLOW: OS access is allowed, but protected by a SAProuter password.
RED: OS access is allowed and there is no SAProuter password used.

RED:
Evaluated Risk - HIGH
You allow permanent direct OS access (port 23, 1503, or 5601) by means of the SAProuter. Unfortunately, you do not use SAProuter passwords. This is a very critical setting in your SAPROUTTAB.
Recommendation: Only open these destination services if the SAP Support Team requests you to do so, and close them again after the problem has been solved. These services might still be open, because you forgot to close them after the problem was solved. If you decide to open these destination services permanently, at least ensure that only SAP can access your systems, and that these lines of communication are protected by SAProuter passwords.
Implementation: After you have found out what communication really takes place by means of the SAProuter, you can update the SAPROUTTAB, and either restart the SAProuter or use option "-n" to activate the new SAPROUTTAB without canceling all the active connections.

YELLOW:
Evaluated Risk - MEDIUM
You allow permanent direct OS access (port 23, 1503, or 5601) by means of the SAProuter. Fortunately, you use SAProuter passwords.
Recommendation: Only open these destination services if the SAP Support Team requests you to do so, and then closed them after the problem has been solved. These services might still be open, because you forgot to close them after the problem was solved.
Implementation: After you have found out what communication really takes place by means of the SAProuter, you can update the SAPROUTTAB, and either restart the SAProuter or use option "-n" to activate the new SAPROUTTAB without canceling all the active connections.
Do not grant permanent direct OS access (service 23, 1503, or 5601) in the SAPROUTTAB as a general setting as this is critical from a security point of view. Only activate it if the SAP Support Team requests you to do so, and then deactivate it after the problem has been solved. If you have to activate this setting, at least set a SAProuter password, and restrict the source IP address to SAP.

9.1.8 Access from SAP via the SAProuter Doesn't Require SAProuterPassword (0553)

Purpose
To check that every connection from SAP to the customer via the SAProuter is set up with a SAProuter password. Otherwise, the open connection could be used by anybody (at SAP) to route to the customer.
Procedure
Check whether a SAProuter password is maintained for any connection from SAP to the customer system.

Risk Rating
Set the rating manually as follows:
GREEN: A SAProuter password is maintained for every connection from SAP to the customer.
YELLOW: At least one connection from SAP to the customer system does not contain a SAProuter password.

Evaluated Risk - MEDIUM
At least one connection from SAP to your systems does not require a SAProuter password.
Recommendation: In the SAPROUTTAB, add SAProuter passwords for all connections from SAP to your systems.
Implementation: After you have made the changes in your SAPROUTTAB, you can either restart the SAProuter or use option "-n" to activate the new SAPROUTTAB without canceling all the active connections.
Every connection from SAP to the customer by means of the SAProuter must be set up with a SAProuter password. Otherwise, the open connection can be used by anybody (at SAP) to route to the customer.

9.1.9 SAProuter Connections Are Not Logged (0554)

Purpose
To check whether logging is activated for SAProuter connections. You can track the root cause of security problems only if logging is activated for SAProuter connections.

Procedure
Since this option is activated as the command line option of the SAProuter, ask the customer to set this. Logging is activated with the parameter "-G" in the SAProuter command line. The next parameter is then the file name of the log file.

Risk Rating
Set the rating manually as follows:
GREEN: A log file is activated by using the "-G" option.
YELLOW: The parameter "-G" is not in use and therefore the log file is not currently active.

Evaluated Risk - MEDIUM
Recommendation: Since the SAProuter supports external connections into your network, we recommend that you log all connections, so that incidents can be tracked afterwards. Restart your SAProuter with the "-G" option and a log file name. Then check the created file on a regular basis.
You can track the root cause of security problems only if you activate logging for SAProuter connections.

9.1.10 Activities of the OSS Users Are Not Logged in the Security Audit Log (0533)

Purpose
To check whether activities of the SAP OSS user are recorded in the Security Audit Log to ensure that there is enough information to track security incidents.

Procedure
The customizing of the Security Audit Log is checked.

Risk Rating
The rating is set automatically as follows:
GREEN: The unsuccessful activities of the SAP OSS user in all clients are logged in the audit log.
YELLOW: The audit log is not enabled or only successful events are logged.

Evaluated Risk - Medium
Recommendation: Log the activities of the OSS user in the Security Audit Log.