# User Guide CheckAud® for SAP Systems 2025.2

Document version: UG.CASA.2025.2.1609.01

A product of IBS Schreiber GmbH

ibs Schreiber

# Table of contents

# Chapter I - Introduction

# I Introduction

## I - 1 Use and benefits of CheckAud 2025.2

CheckAud for SAP Systems was developed with the aim of making authorization concepts more trans-parent and easier to evaluate, and of enabling you to audit security-sensitive areas of an SAP system. The tool is primarily used for internal auditing by companies or by external auditors to technically and functionally map the auditing job in question. Many of the functions provided in CheckAud® have been designed and developed for use by auditors.

Today's requirements for SAP system security necessitate additional (preventive) checks that must be performed by the specialist departments involved. With that in mind, CheckAud finds application in areas such as system administration or authorization management, or in the respective specialist departments such as financial accounting or materials management. These users sometimes have a different focus than the auditor and therefore have different requirements for CheckAud. In addition, the very technical and detailed results of the evaluation of the SAP system authorization structure must be prepared in a suitable form for management level so that potential security risks can be identified quickly and respond-ed to appropriately. This management view is also available in CheckAud, allowing you to keep the downstream manual preparation and assessment of the results to a minimum.

## I - 2 CheckAud 2025.2 as a part of risk management

CheckAud is designed for broad deployment within the company. The auditing software is not only in-tended for internal auditing; instead, it is intended for use in all business areas that influence the assign-ment of authorizations in the SAP system (functionally and technically) and therefore system security.

Risk management should include the definition of risks to compliance requirements and company re-quirements (for example, separations of function) for all the areas of business of a company, the effects of these risks and suitable preventive and corrective measures. This information is taken into account both during the initial configuration of CheckAud and during its regular use.

CheckAud therefore constitutes a technical control instrument for risk management. Once configured and regularly maintained, CheckAud becomes a central risk management component in SAP systems.

# Chapter II - CheckScan 2025.2 (Scan module)

# II CheckScan 2025.2 (Scan module)

## II - 1 User interface

The following figure shows the CheckScan 2025.2 user interface:

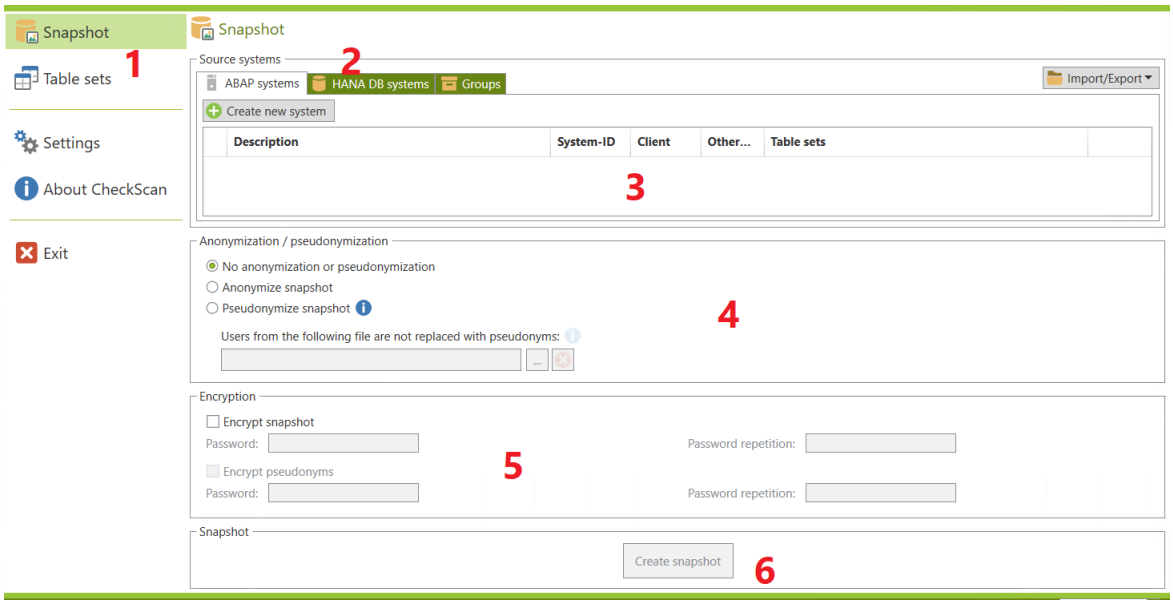



**Figure 1 - User interface CheckScan**

| | | |
|---|---|---|
| 1. | | Main menu |
| | Snapshot | Main window for managing the SAP system connections / HANA database connections |
| | Table Sets | Configuration area for the SAP tables to be exported / HANA database tables |
| | Settings | Global program settings for CheckScan |
| | About CheckScan | License and version information |
| | Exit | Close CheckScan |
| 2. | | SAP system connections / HANA database connections, tabs for displaying the systems as a list or in groups |
| 3. | | Display of the maintained SAP system connections / HANA database connections as a list or in groups |
| 4. | | Anonymization or pseudonymization for the snapshot, optional |
| 5. | | Snapshot encryption, optional encryption of pseudonymization file |
| 6. | | Snapshot creation/Display of the current snapshot creation status |

# II - 2 Table Sets

## II - 2.1 ABAP Systems

In the *Table Sets* menu item, the Auth table set is specified by default. This table set con-tains all the relevant SAP tables for analyzing the assigned SAP authorizations. It is therefore vital that CheckScan has access to this tables in order to create a snapshot. No changes can be made to this table set. Apart from the obligatory AUTH table set, additional optional tables sets are available. These tables include information about the BW, FI, HCM, ISU, MM, SD and Basis modules and are not necessarily required to perform the authorization checks.

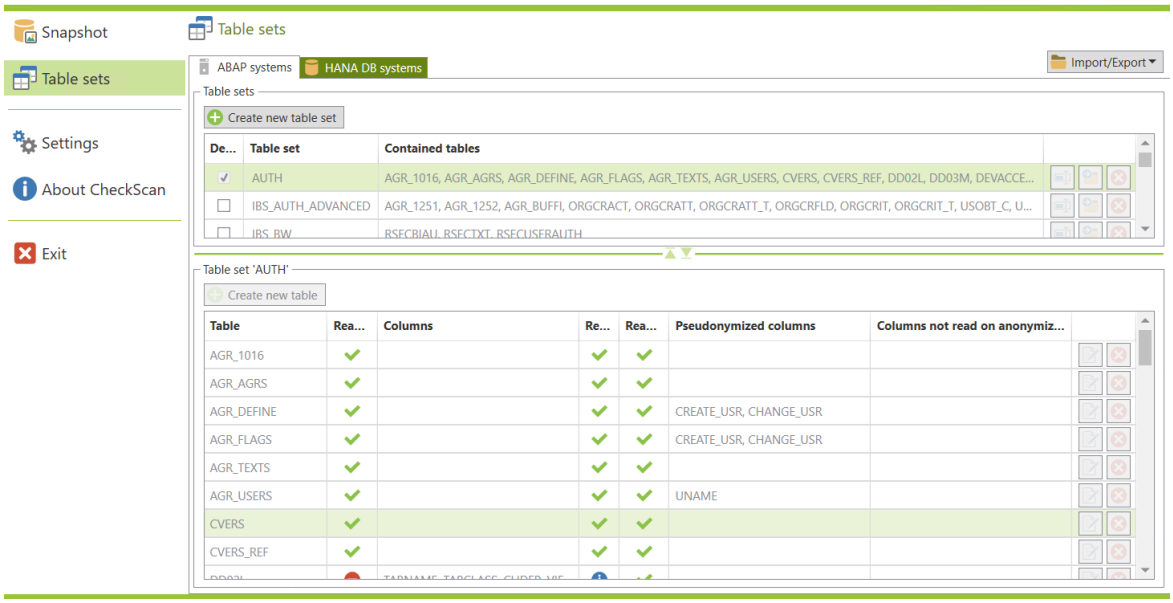
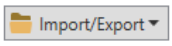



**Figure 2 - Standard table set Auth**

When you select a table set in the selection window, the lower area of the window displays the details of the SAP tables included in the table set. It prepares the following table view to do so:

| | |
|---|---|
| *Table* | Name of the SAP table to be included in the scan |
| *Read all columns (except the specified ones)* | Indicates whether the system is to consider all the columns from the specified SAP table (no: ⛔, yes: ✔) |
| *Columns* | If you do not choose to consider all table columns, you can specify explicitly whether certain table columns are included or excluded |
| *Read table completely* | SAP tables that are read under certain conditions exist in predefined table sets. The criterion for reading an SAP table is indicated using the ℹ icon. When you move the mouse cursor onto the icon, the defined criterion for this table is displayed. |
| *Read on anonymization and pseudo-nymization* | Columns in the SAP table that are still read even when anonymization and pseudonymization are activated |

| | |
|---|---|
| *Pseudonymisierte Spalten* | Columns that are shown in pseudonymized form in the table display |
| *Columns not read on anonymization and pseudonymization* | If anonymization and pseudonymization are enabled, the defined columns are skipped while reading out the table |

The 

button can be used to load or save internal table sets.

Detailed information about SAP tables / table sets regarding data protection an data deletion can be found in the separate CheckAud Data Protection Guide.

## II - 2.2 HANA DB Systems

In the *Table Sets* menu item, the Auth table set is specified by default. This table set con-tains all the relevant HANA database tables for analyzing the assigned HANA database authorizations. It is therefore vital that CheckScan has access to this tables in order to create a snapshot. No changes can be made to this table set. Apart from the obligatory AUTH table set, additional optional tables sets are available. These tables include information about the BW, FI, HCM, ISU, MM, SD and Basis modules and are not necessarily required to perform the authorization checks.

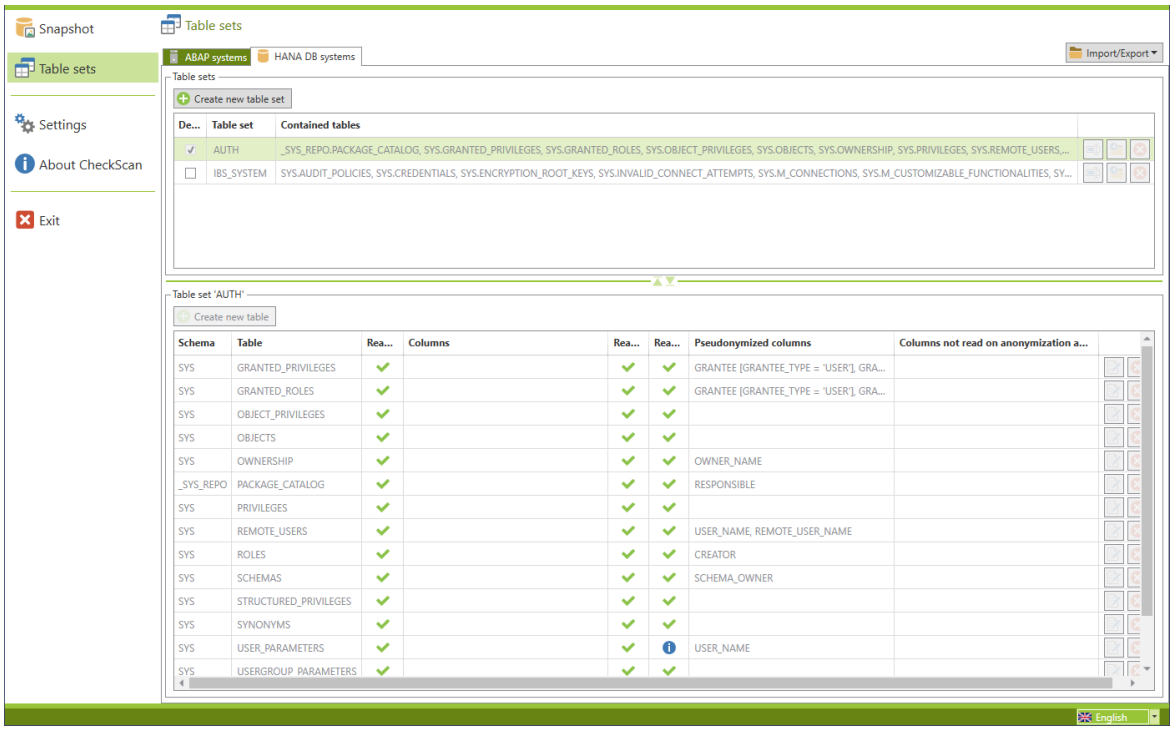
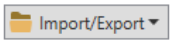



**Figure 3 - Standard table set Auth**

When you select a table set in the selection window, the lower area of the window displays the details of the HANA database tables included in the table set. It prepares the following table view to do so:

| | |
|---|---|
| *Schema* | Name of the Schema in which the needed HANA database table is located |
| *Table* | Name of the HANA database table to be included in the scan |

| | |
|---|---|
| *Read all columns (except the specified ones)* | Indicates whether the system is to consider all the columns from the specified HANA database table (no: ⛔, yes: ✔) |
| *Columns* | If you do not choose to consider all table columns, you can specify explicitly whether certain table columns are included or excluded |
| *Read table completely* | HANA database tables that are read under certain conditions exist in predefined table sets. The criterion for reading a HANA database table is indicated using the ℹ icon. When you move the mouse cursor onto the icon, the defined criterion for this table is displayed. |
| *Read on anonymization and pseudonymization* | Columns in the HANA database table that are still read even when anonymization and pseudonymization are activated |
| *Pseudonymisierte Spalten* | Columns that are shown in pseudonymized form in the table display |
| *Columns not read on anonymization and pseudonymization* | If anonymization and pseudonymization are enabled, the defined columns are skipped while reading out the table |

The 

button can be used to load or save internal table sets.

Detailed information about HANA database tables / table sets regarding data protection an data deletion can be found in the separate CheckAud Data Protection Guide.

## II - 2.3 Creating your own table set

Use the 

button to create your own table set. After assigning a name to the additional table set, you can use the 

button to add a new table for CheckScan to read during the scanning process. You can use the technical name to show/hide, anonymize or pseudonymize specific columns.

The following example shows the additional readout of the table T001L of an ABAP system:

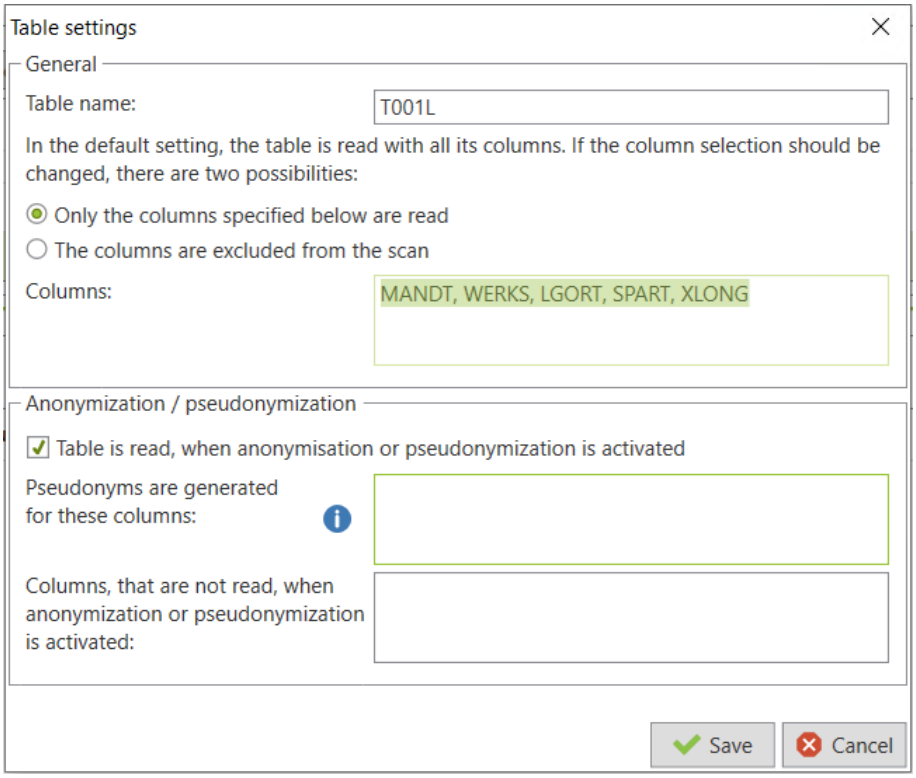



**Figure4 - Including specific columns in the readout**

Once the snapshot has been imported to CheckAud, the table T001L can be shown in the table display. The criterion, which must be defined in the table settings (Tabellen-Einstellung), causes only the defined columns to be displayed in the table display. The specified columns are separated by a comma.

**Note 1**: If no column entries have been chosen, an error occurs when you start the scan.

**Note 2**: The RFC interface user created in the SAP system (scan user) must have the authorization to read the specified table in your table set. If the user does not have this authorization for the specified table, an error occurs when you start the scan.

The example below shows the additional readout of the table T001L of an ABAP system; in this case, specific table columns are now excluded from the scan:

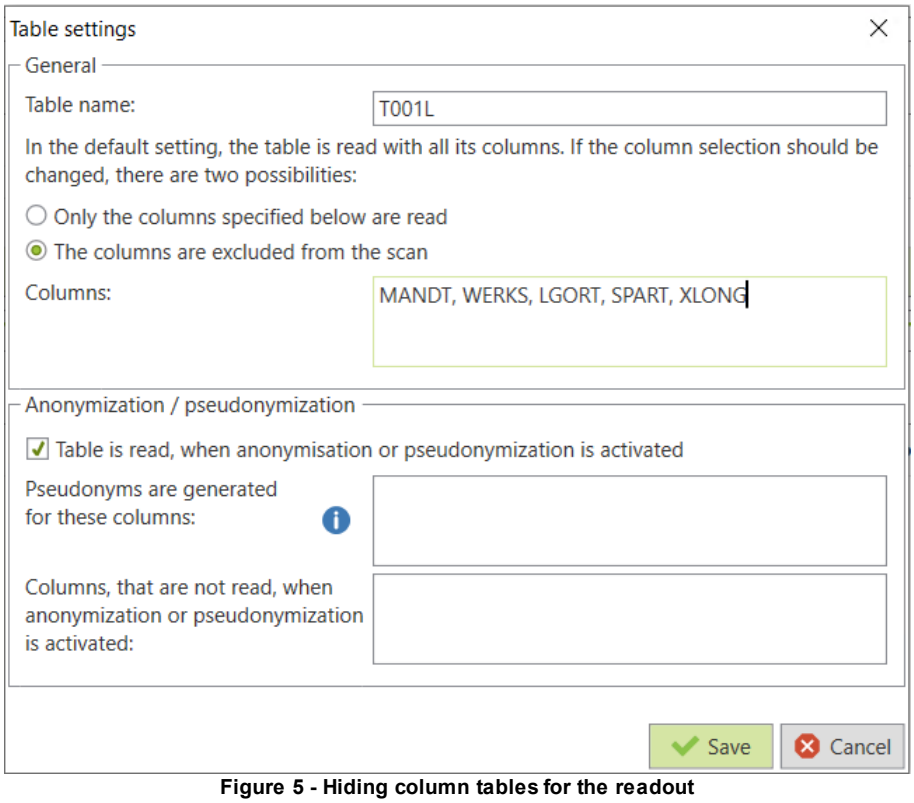



**Figure 5 - Hiding column tables for the readout**

Once the snapshot has been imported to CheckAud, the table T001L can be shown in the table display. The criterion, which must be defined in the table settings (Tabellen-Einstellung), causes only the specified columns to be excluded from the table display.

**Note:** If no column entries are defined, the snapshot contains all columns for the specified table.

The example below shows the additional readout of the table T001L of an ABAP system; in this case, specific table columns are now anonymized/pseudonymized:

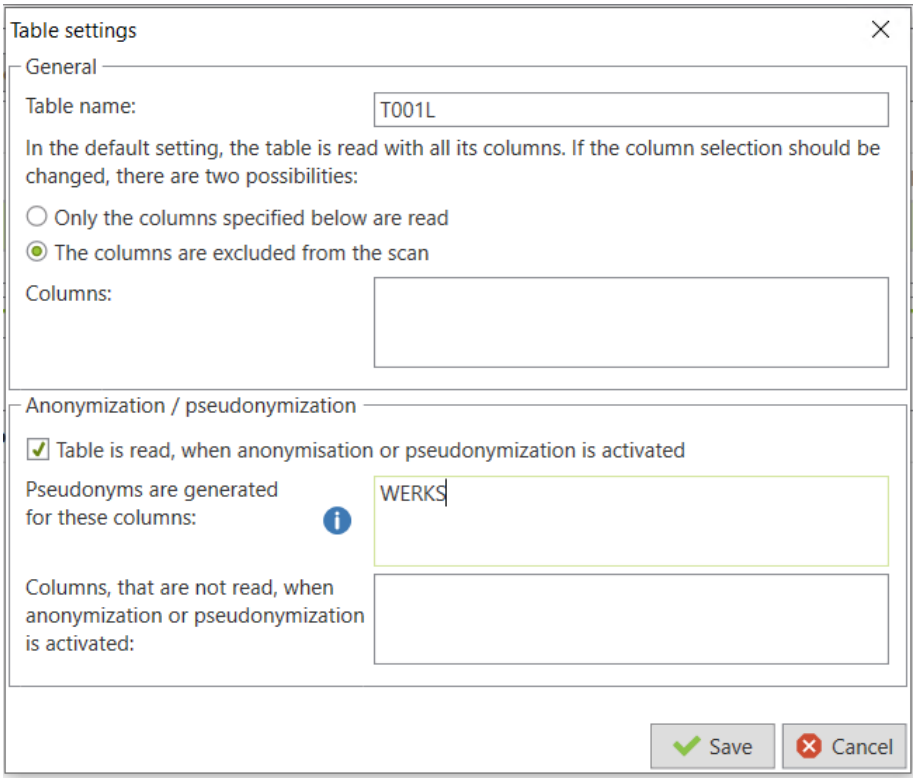



**Figure 6 - Anonymizing/pseudonymizing specific columns in the readout**

When anonymization/pseudonymization is enabled, the values in the column WERKS are now concealed in the CheckAud table display.

The example below shows the additional readout of the table T001L of an ABAP system; in this case, specific table columns are now skipped when anonymization/pseudonymization is enabled:

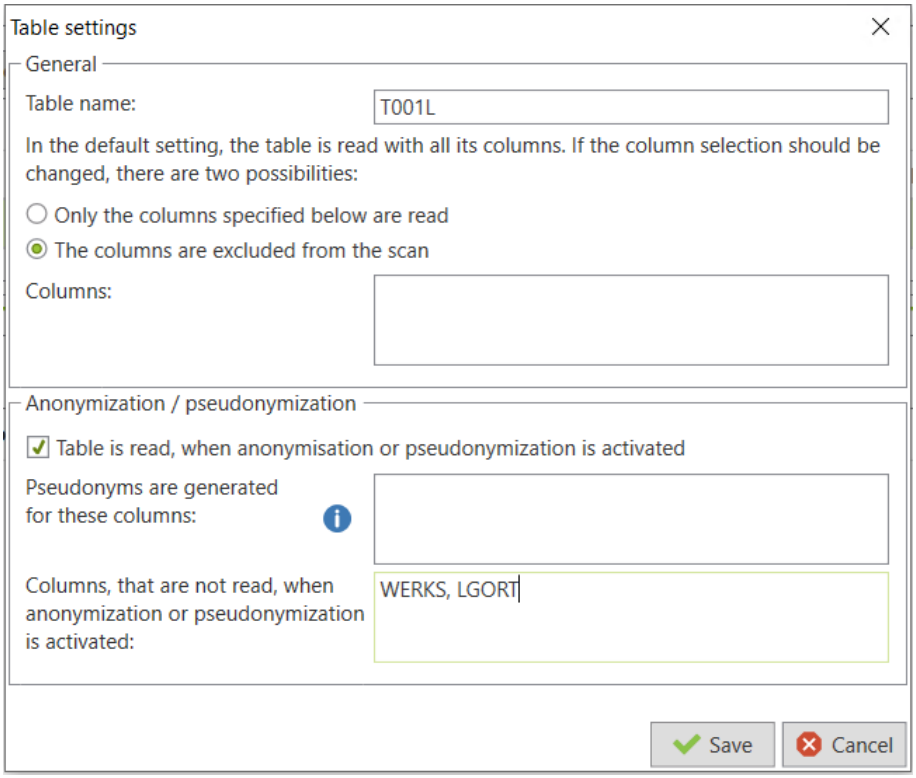



**Figure 7 - Skipping columns in the readout when anonymiza-tion/pseudonymization is enabled**

The contents of the columns WERKS and LGORT are shown without entries in the CheckAud table display when pseudonymization or anonymization is activated.

Also additional table sets for a HANA DB systems can be build that way. Please note, that the database schema has to be defined in that case:

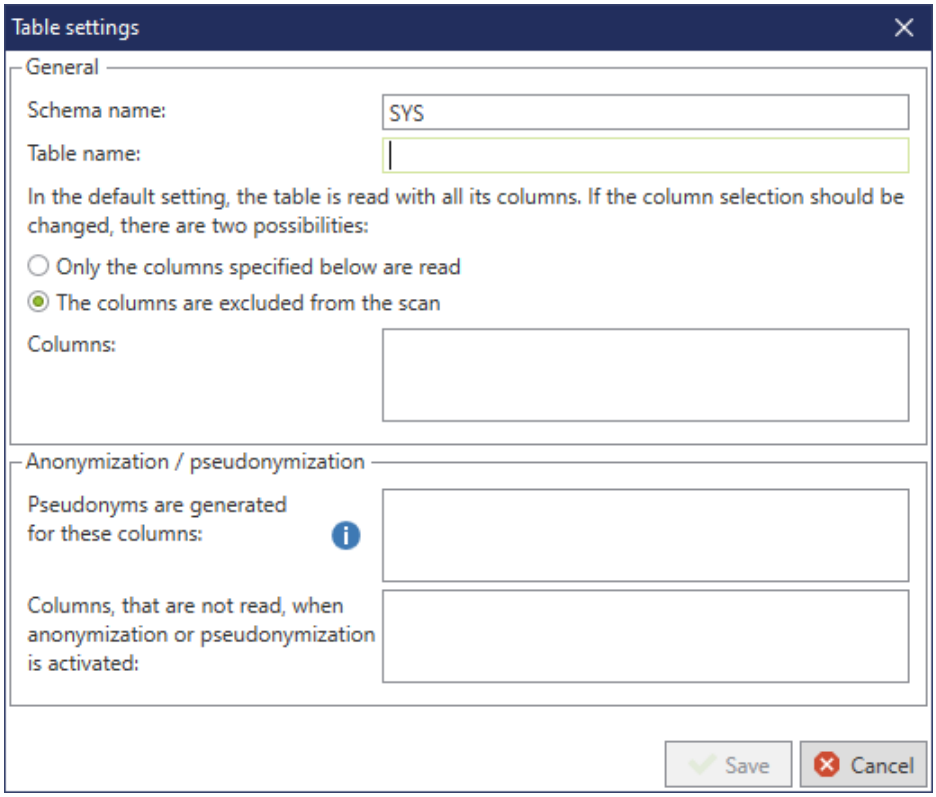



**Figure 8 - Reading out tables of a HANA DB system**

## II - 2.4 Note on field with unsupported data types

Among others, the function module RFC_READ_TABLE is used to read tables. This function module is for reading out all the data types in the tables available in the SAP system. The following table types should not be read with your own table set using CheckScan:

- DEC, CURR
  - in many cases, the values for these types are not properly returned, so fields of this type cannot be meaningfully analyzed. However, the readout also does not fail, which means it is not absolutely necessary to exclude the fields.
- RAW
  - The data from RAW-type fields cannot be fully read (only the first half of the data is returned). From a length of more than 255 characters, a reading is generally not possible.
- STRING, SSTRING, RAWSTRING
  - Tables with fields that contain these types of data cannot be read due to the variable length. The reading fails even if the columns are explicitly excluded.

# II - 3 Settings

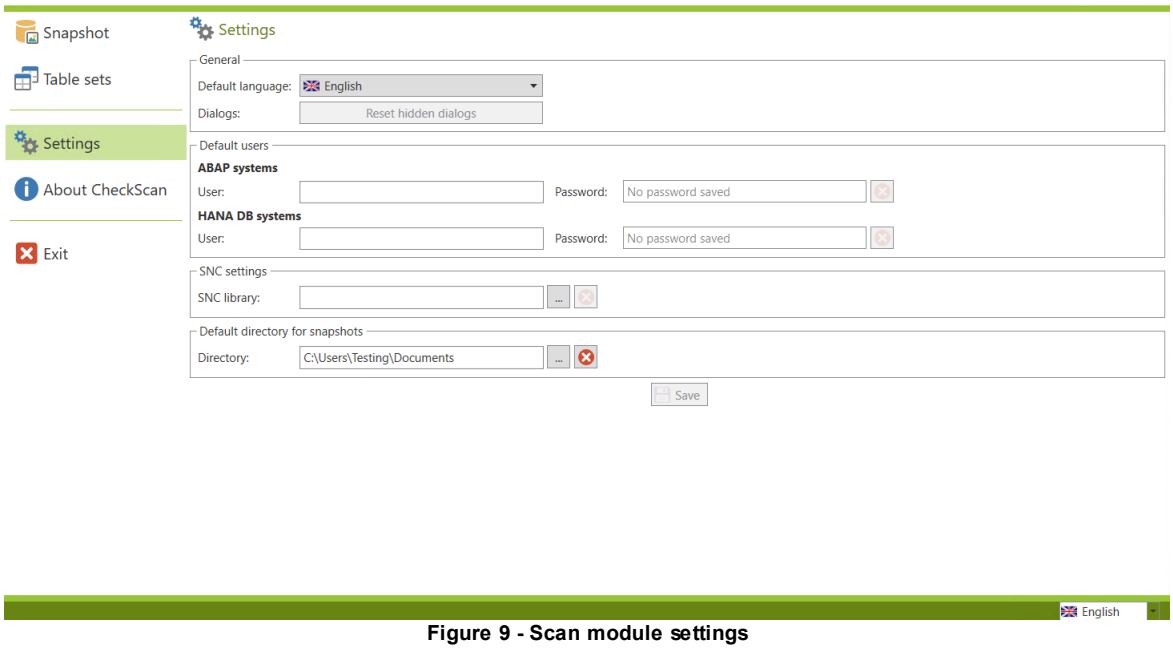



**Figure 9 - Scan module settings**

| | |
|---|---|
| *Default language* | Determines the language in which you want the scan module to start. |
| *Dialogs* | Some Dialogs can be hidden with the option *Do not show this notice in the future* with this button, hidden dialogs will be shown again. |
| *ABAP systems standard user* | Login information for a SAP standard user is entered here, which you have the option of using for the system connections. This means you do not have to enter the communication user's details for each system connection. |
| *HANA DB standard user* | Login information for a HANA database standard user is entered here, which you have the option of using for the system connections. This means you do not have to enter the communication user's details for each system connection |
| *SNC library* | SNC (Secure Network Communications) is used to guarantee security by means of encryption between client and server components. CheckScan automatically detects whether the SAP Secure Login Client is already installed on the workstation and automatically enters the SNC library path. CheckScan needs access to the file sapcrypto.dll in order to establish the connection using SNC. This file is saved in the program directory of the SAP Secure Login Client. If it is not possible to detect the file automatically, you can enter the path manually. If you are not using an SNC connection, then the SNC library is not necessary. |
| *Default directory for snap-shots* | Determines the path in which the dialog window for saving the snapshots is to be opened. |

# II - 4 Information about CheckScan

## II - 4.1 Viewing / installing a license


The button displays the license in detail. You can use the 

button to update or renew the license. The procedure is analogous to the initial installation of the license file.

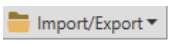
## II - 4.2 Using the scan module without a license

The scan module can be used to read out SAP source systems without a license. For example, this may be necessary as part of the preparations for an external audit by IBS Schreiber GmbH. Snapshots that are generated by an unlicensed scan module are safeguarded through automatic encryption. These snapshots can only be imported and evaluated by IBS Schreiber GmbH employees as part of an audit.

# II - 5 Creating a new system connection (ABAP)

**Note:** To create system connections, you need detailed information about the SAP source systems to be exported (TCP/IP address, DNS address or SAProuter string, message server, server group, client, sys-tem number, etc.). This information should be available from SAP Basis administration.

You can use the button 

to create a new connection to a SAP source system. Previously created source systems can be exported or imported using the 

button. In this way, information about SAP source systems can be exchanged between different scan module installations.

This button can still be used to load the *SAPLOGON.INI* of an existing SAP LogOn installation. In the process, the connection information available in *SAPLOGON.INI* is copied and must only be supplemented by the client or the SAP communication user's logon information.

The following dialog box for establishing a new system connection is displayed:

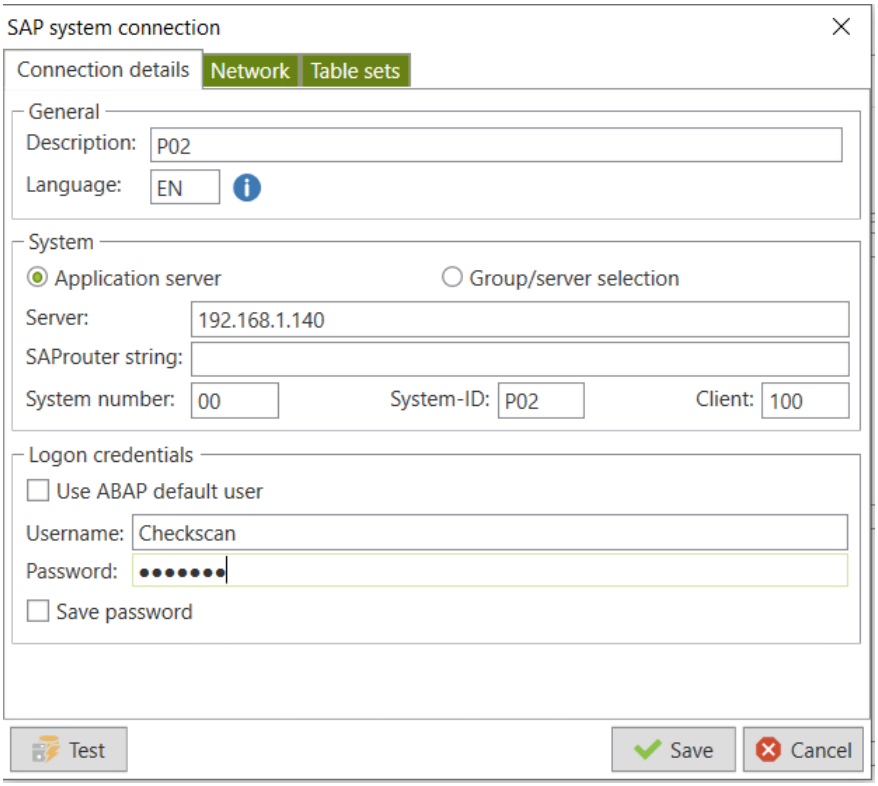
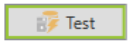



**Figure 10 - Entering the connection information for an SAP system**

| | |
|---|---|
| *Description* | User-defined description of the source system to be created |
| *System* | Choose between a connection via application service or groups/server selection |
| *Server* | TCP/IP address or DNS address of the SAP host |
| *SAProuter-String* | Alternative connection via the SAProuter string |
| *System number* | Instance number of the SAP source system |
| *System-ID* | System designation of the SAP source system |
| *Client* | Client to be read out from the SAP source system |
| *Credentials* | Name and password of the SAP communication user for logging the scan module onto the source system (alternatively, the SAP standard user saved to the settings can be enabled here using the flag) |
| *Safe password* | As long as this flag has not been enabled, each time a snapshot is created, a prompt for the SAP communication user's password will appear, if activated, the password will be stored encrypted |

You can use the button 

to check whether it is possible to connect to the source system using the saved information.

## II - 5.1 Creating new SAP system connection via SNC

To enable SNC (Secure Network Communication), the SNC library is required and can only then be enabled. In order to create the connection, the SNC server name must be defined. The SNC user name (SNC-Name des Benutzers) is optional and is not a mandatory field. After selecting the correct security level, the connection can now be tested.

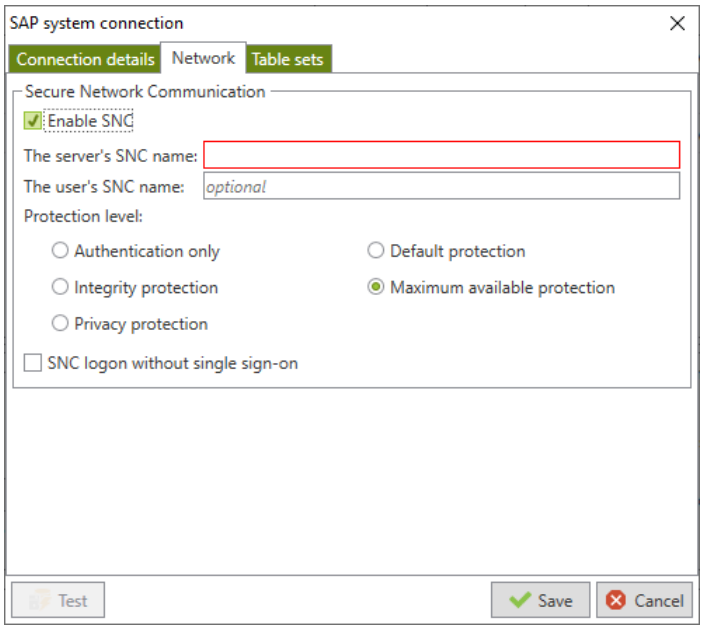



**Figure 11 - Connecting via SNC**

## II - 5.2 Adding additional table sets

On the Table sets tab, you can select additional table sets that are also relevant to this system connection in addition to the mandatory table set AUTH. The table sets:

- IBS_AUTH_ADVANCED,
- IBS_BW,
- IBS_FI,
- IBS_GDPR
- IBS_HCM,
- IBS_ISU,
- IBS_MM,
- IBS_SD and
- IBS_SYSTEM

are provided as predefined additional options. Your own table sets are displayed dynamically in the main menu item Table Sets (Tabellen-Sets) and on this tab.

The figure below shows the additional selection of the table set *IBS_AUTH_ADVANCED*:
:

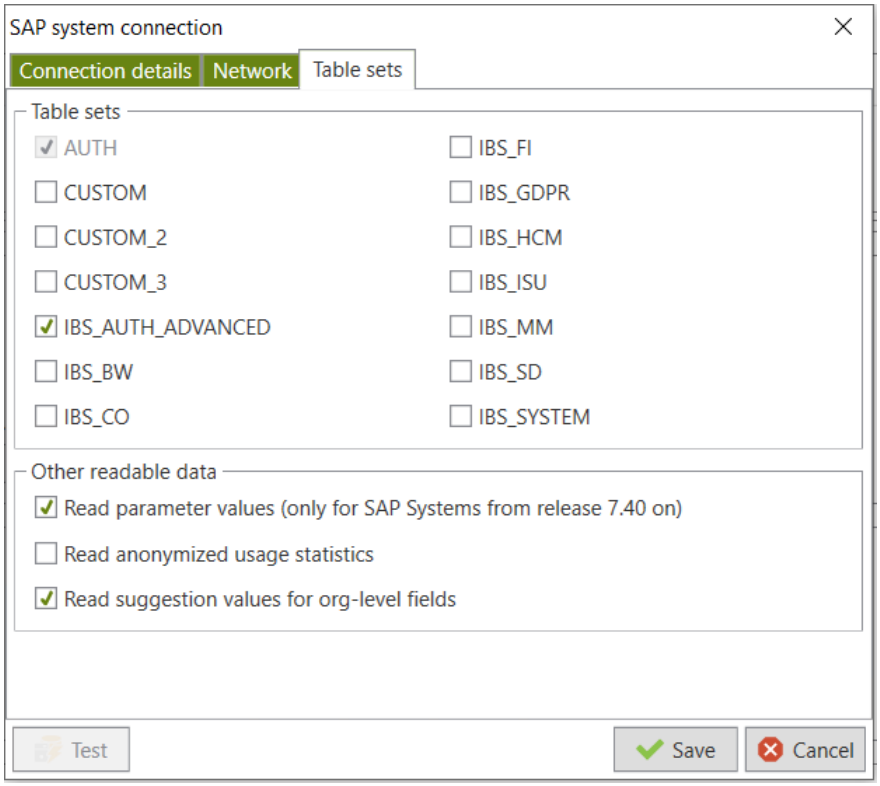



**Figure 12 - Selecting additional table sets**

Use the *Save* button to save the new system connection. In the *Table Set* column in the SAP source system overview, you can see which table sets have been enabled.

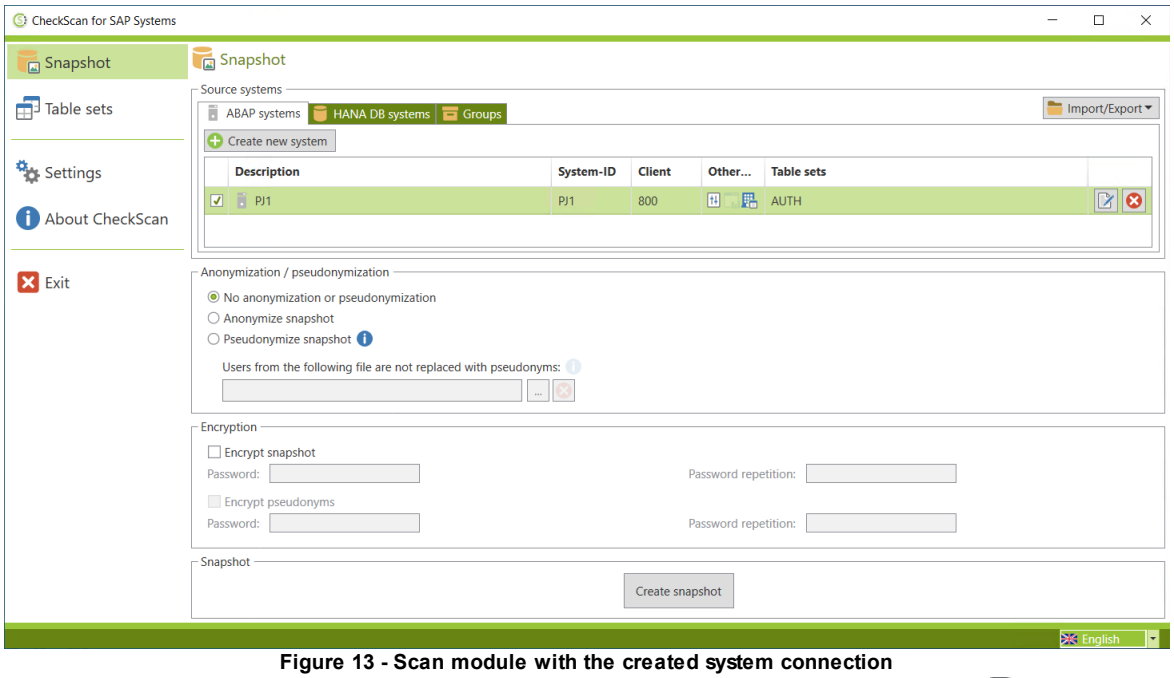



**Figure 13 - Scan module with the created system connection**

System connections that have already been created can be edited with the button and deleted with

## II - 5.3 Reading out parameters

In addition to table sets, the Table sets tab also contains additional options for the information to be read out:

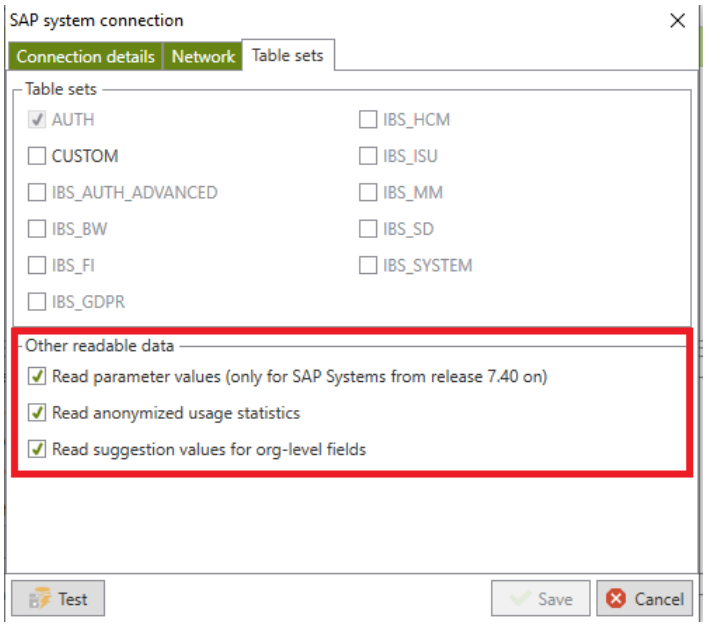



**Figure 14 - Reading out parameter values**

To check the parameters of an SAP system in CheckAud, the parameters must be read out. Readouts of parameter values are activated by default in CheckScan. As well as the existing authorizations for the AUTH table set, additional authorizations are required to read out the parameter values. You can read out system parameters only with SAP Release 7.40 or later. For older releases, it is not possible to read out parameter evaluations in CheckAud even when the option is set.

## II - 5.4 Reading out default values for org levels

In addition to table sets, the Table sets tab also contains additional options for the information to be read out:

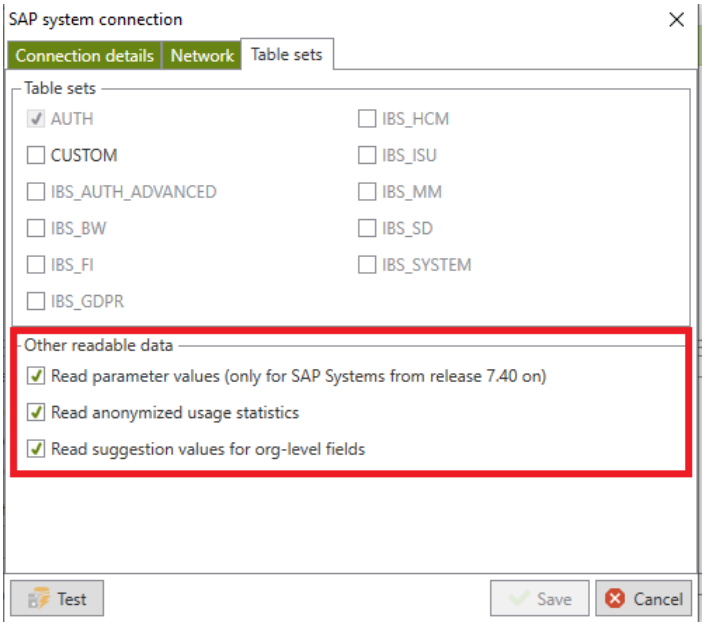



**Figure 15 - Reading out default values for org levels**

To be able to use the default values for organization levels (e.g. for company code BUKRS) in CheckAud, these values must also be read out. Readouts of the default values for org levels are activated by default in CheckScan. Additional authorizations are required on top of the existing authorizations for the AUTH table set.

**Note:** If the readout of the SAP system results in longer runtimes, this option for reading out the org levels can be disabled to improve the runtimes. As a result, however, the default values for org levels cannot be provided during the evaluation and must be entered manually.

## II - 5.5 Reading out anonymized user statistics

It is possible to read out the SAP user statistics in an anonymized way. With these information it is possible to do evaluations and getting results about the used transactions. That could be helpful in case of redesigning the authorization concept.

To read out the user statistics, you have to activate the corresponding flag in the Scan module:

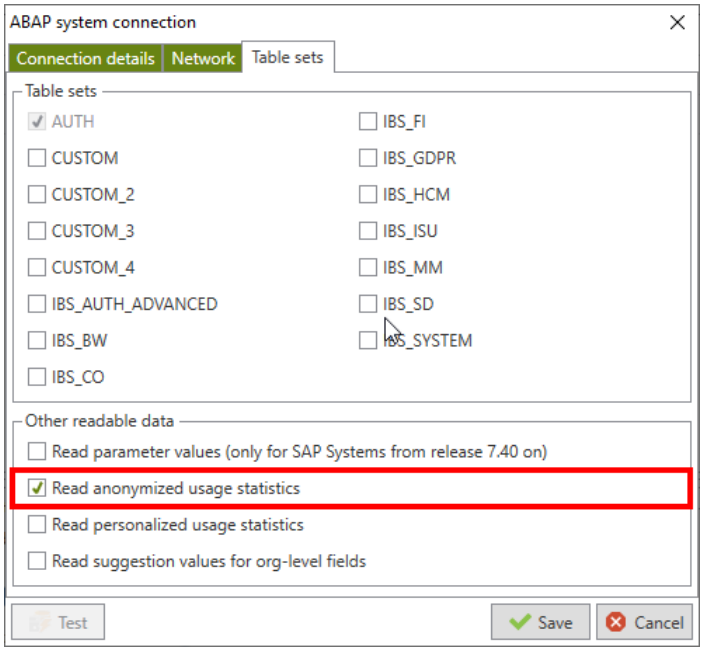



**Figure 16 - Read anonymized user statistic**

**Note:**

- the user statistic will be fully anonymized, there won't be any user names in the statistic informationen (no control of user behavior possible))
- IBS Schreiber GmbH delivers a preconfigured role for reading out the user statistics

With the user statistics read out, several tables are accessable for evaluation in the toolbox *Tables:*

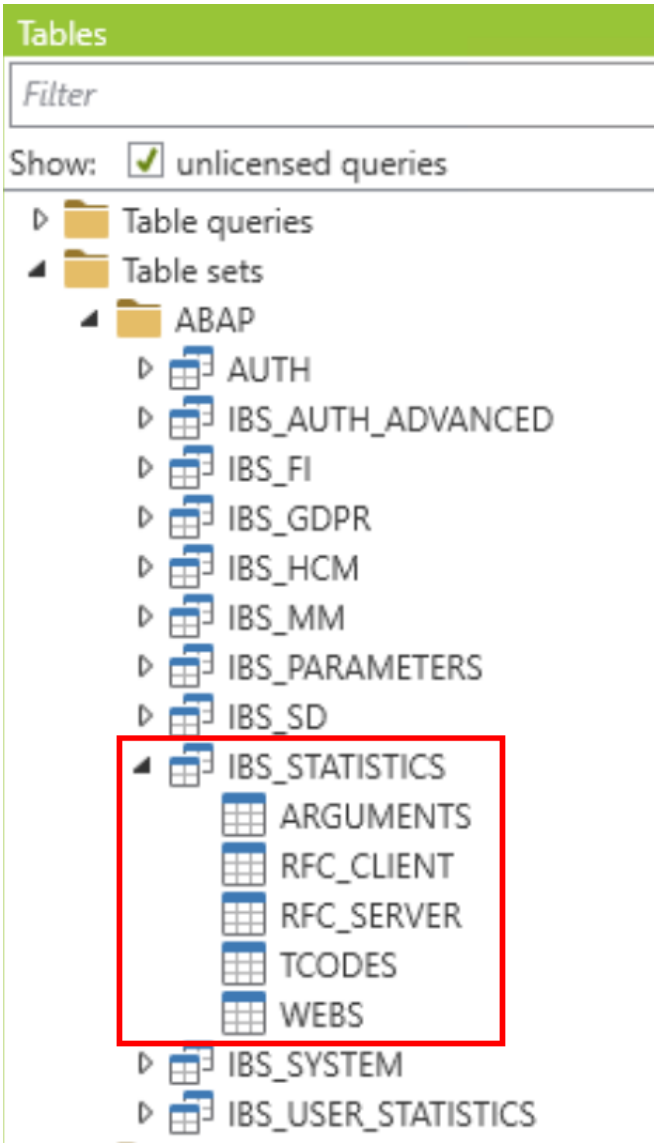



**Figure 17 - Accessable tables for user statistics**

## II - 5.6 Read out personalized user statistics

It is also possible to read out the SAP user statistics in personalized form. With this information it is possible to do evaluations and getting results about the used transactions per user. That could be helpful in case of redesigning the authorization concept.

To read out the user statistics in personalized form, you have to activate the corresponding flag in the Scan module:

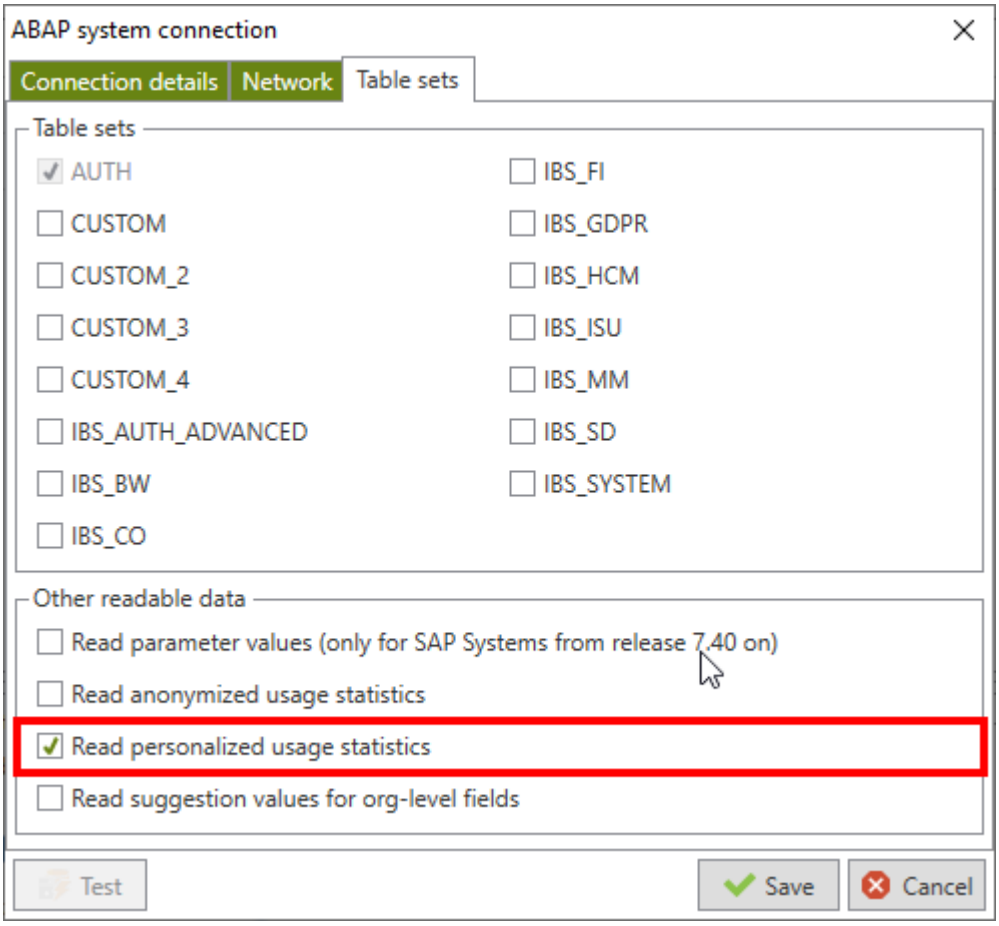



**Figure 18 - Read out personalized usage statistics**

## II - 6 Creating a new system connection (HANA DB)

**Note:** To create system connections, you need detailed information about the HANA source database to be exported (TCP/IP address, DNS address, instance number, etc.). This information should be available from SAP Basis administration.

You can use the button Create new system to create a new connection to a HANA source database. Previously created source systems can be exported or imported using the Import/Export button. In this way, information about HANA source database can be exchanged between different scan module installations.

This button can alsol be used to load the conecction information from the SAP HANA Cockpit or the SAP HANA Studio.In the process, the connection information available from the SAP HANA Cockpit/Studio is copied and must only be supplemented by the communication user's logon information.

The following dialog box for establishing a new system connection is displayed:

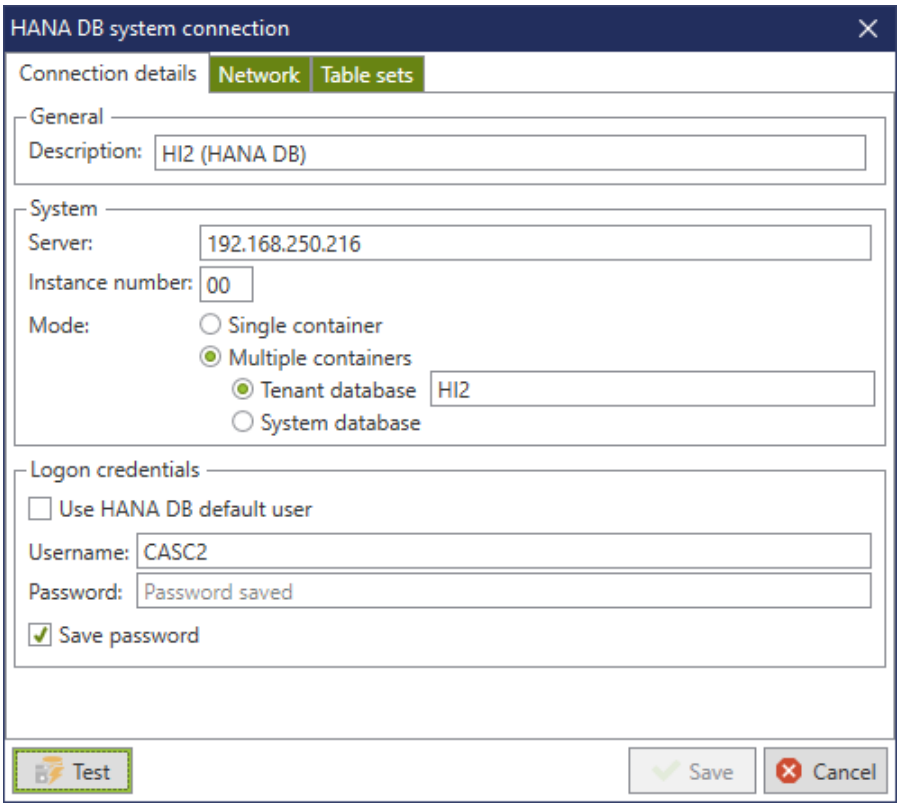



**Figure 19 - Entering the connection information for a HANA database**

| | |
|---|---|
| *Description* | User-defined description of the source system to be created |
| *Server* | TCP/IP address or DNS address of the HANA database |
| *Instance number* | Instance number of the HANA database |
| *Mode* | Mode selection of the HANA database wether the database works as a single container or multiple container. In that case, the tenant hast to be specified |
| *Logon credentials* | Name and password of the communication user for logging the scan module onto the source system (alternatively, the HANA database standard user saved to the settings can be enabled here using the flag) |
| *Save password* | As long as this flag has not been enabled, each time a snapshot is created, a prompt for the communication user's password will appear, if activated, the password will be stored encrypted |

You can use the button 

to check whether it is possible to connect to the source system using the saved information.

## II - 6.1 Encryption of system connection

The access to the HANA database can be encrypted with SSL/TLS, this can be activated in the Tab *Network*:

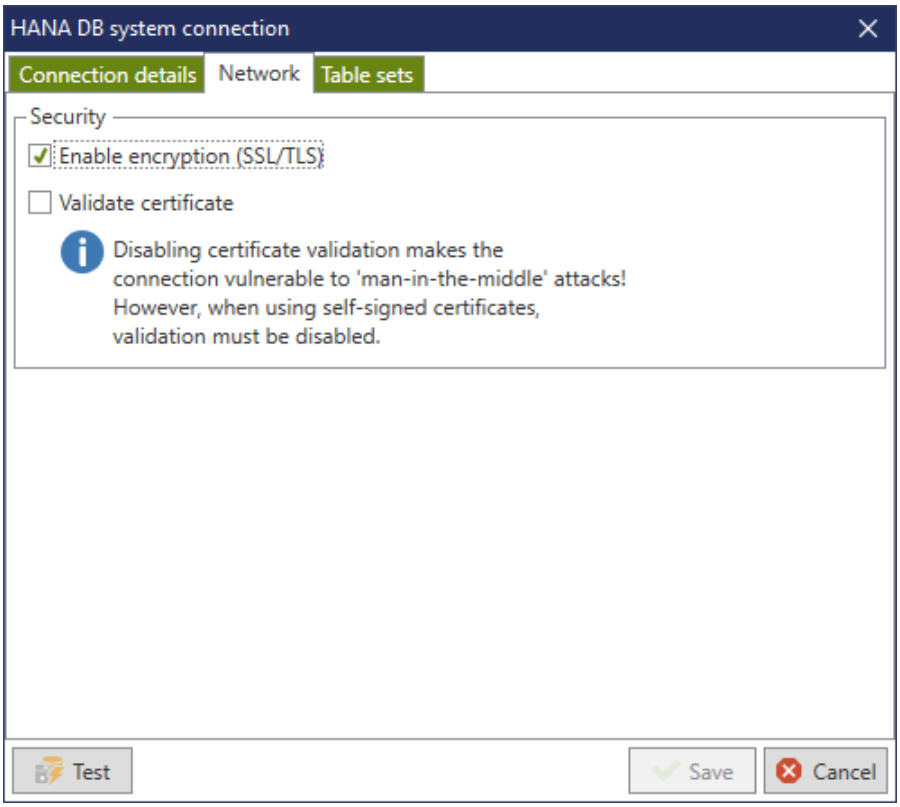



**Abbildung 20 - Aktivierung der SSL/TLS Verschlüsselung**

| | |
|---|---|
| *Enable encryption (SSL/TLS)* | when activated, the connection to the HANA database will be encrypted with SSL/TLS and a certificate is mandatory |
| *Validate certificate* | when activated, the used certificate will be validateted, this will ensure higher security but can lead to failures, when self-signed certificates are used |

## II - 6.2 Adding additional table sets

On the Table sets tab, you can select additional table sets that are also relevant to this system connection in addition to the mandatory table set AUTH. The table sets:

- IBS_SYSTEM

are provided as predefined additional options.

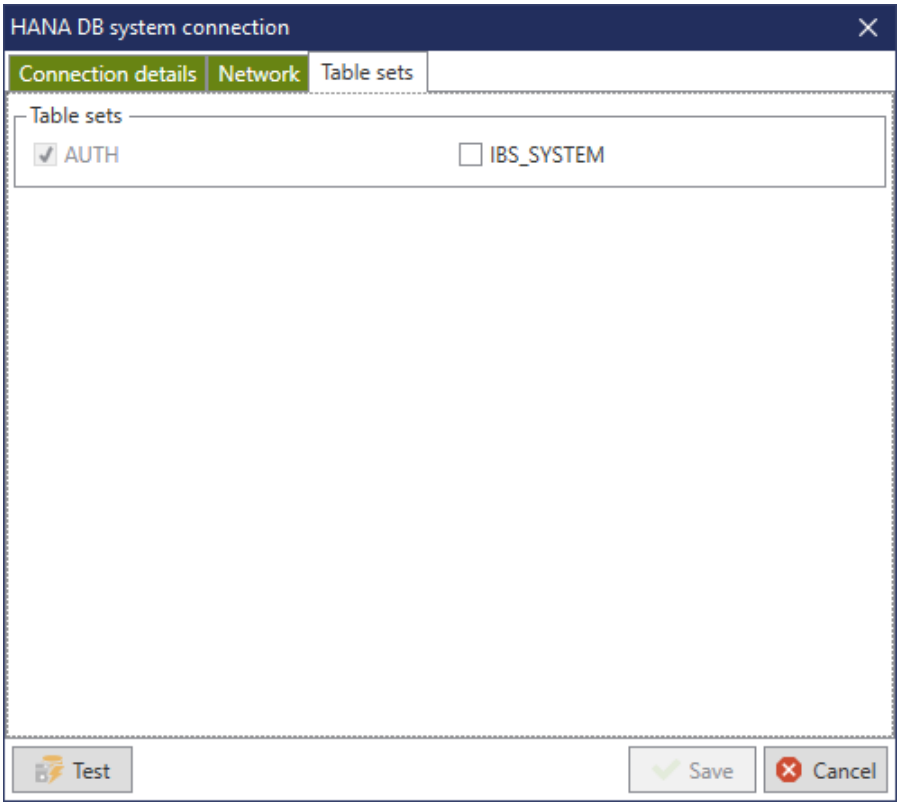



**Figure 21 - Selecting additional table sets**

## II - 7 Anonymization and pseudonymization

Anonymization and pseudonymization are used to conceal personal data in the snapshot.

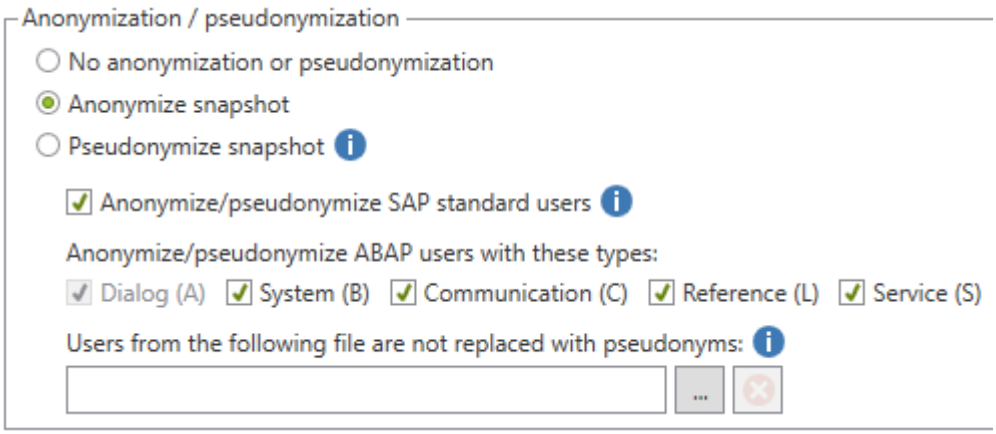



**Figure 22 - Anonymizing the snapshot**

With anonymization, it is not possible to assign them to user names. The user names are stored in anonymized form in the snapshot and cannot be traced back to the original names.

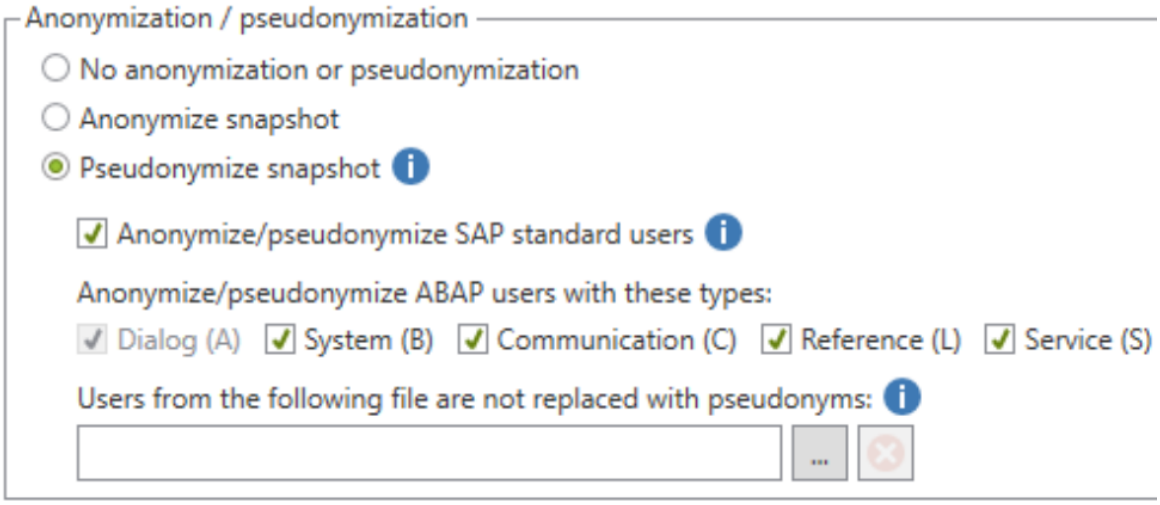



**Figure 23 - Pseudonymizing the snapshot**

With pseudonymization, not only the snapshot, but also an Excel file is created. The pseudonyms and their corresponding user names are stored in the Excel file. This allows the pseudonyms to be matched to the corresponding user names. If necessary, this mapping file can be encrypted for safe storage of personal data.

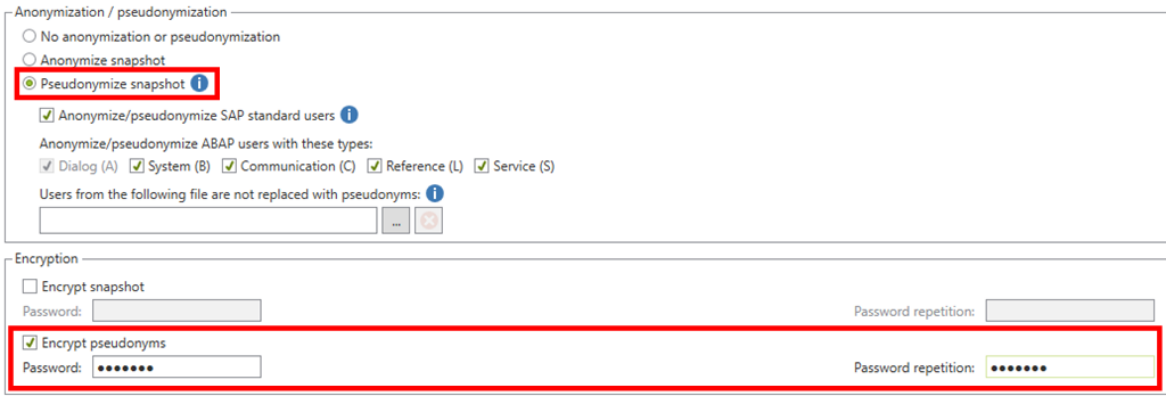



**Figure 24 - Encrypting mapping file**

With anonymization/pseudonymization SAP standard users and all user types except dialog users can be excluded. As a result, these users are displayed in the CheckAud analysis.

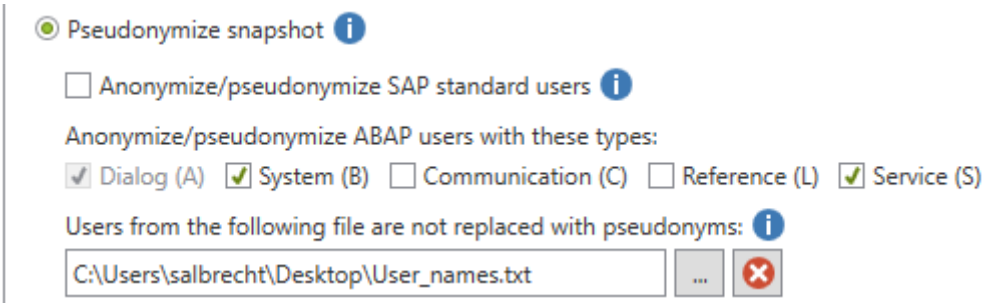
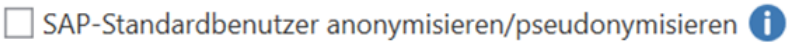


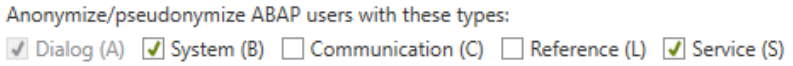

**Figure 25 - Partial pseudonymization**

Users can be excluded from pseudonymization/anonymization (partial pseudonymization/anonymization). As a result, these users are displayed in their plain names in the CheckAud analysis.

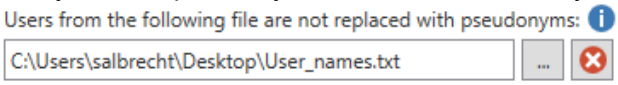
There are different options:

- If the checkbox 

is deactivated, the ABAP resp. HANA DB standard users (SAP*, DDIC etc. or SYS, SYSTEM etc., see for a complete list) are safely excluded from anonymization/pseudonymization and further settings only apply to the remaining users. When activated, however, the standard users are anonymized/pseudonymized, but they can be selectively released from anonymization/pseudonymization again by the following additional options (see examples below).
- It is also possible to select by user type for ABAP users. (Dialog users, however, are always subjected to anonymization/pseudonymization). The following example causes that communication and reference users are not anonymized/pseudonymized, but all other types are:




- In addition, ABAP/HANA DB users stored in a text file can be excluded from anonymization/pseudonymization. The text file may only list one user name in each line.




Combination examples:
1) Default user in plain text + type of default user anonymized/pseudonymized = default user in plain text
2) Default user anonymized/pseudonymized + type of default user in plain text = default user in plain text
3) Default user anonymized/pseudonymized + type of default user anonymized/pseudonymized + default user in text file = default user in plain text

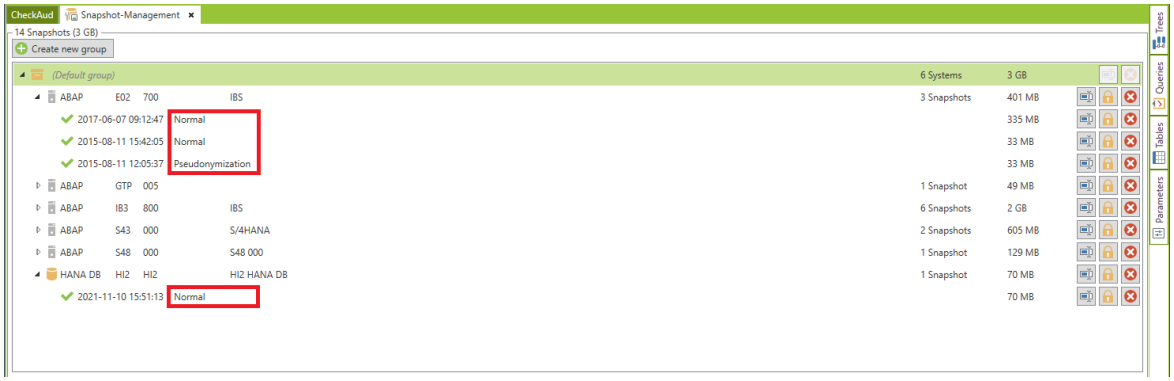



**Figure 26 - Displaying the user mode in snapshot management in the evaluation module**

The relevant user mode for the snapshots can be viewed in snapshot management in the CheckAud evaluation module.

| | |
|---|---|
| *Normal* | No pseudonymization or anonymization |
| *Partial pseudonymization* | Partially anonymized snapshot; inclusion/exclusion of default users, user types and/or users in a text file |
| *Partial anonymization* | Partially anonymized snapshot; inclusion/exclusion of default users, user types and/or users in a text file |
| *Pseudonymization* | Pseudonymized snapshot |
| *Anonymization* | Anonymized snapshot |

Detailed information about anonymization and pseudonymization and about the technical procedures can be found in the separate CheckAud data protection guide.

## II - 8 Group administration of the SAP system connections

As required, the new system connections can be organized into groups to make the sequential readout of the source system easier or organize it more clearly, for example. To group the system connections, use the Groups tab to go to the group view.

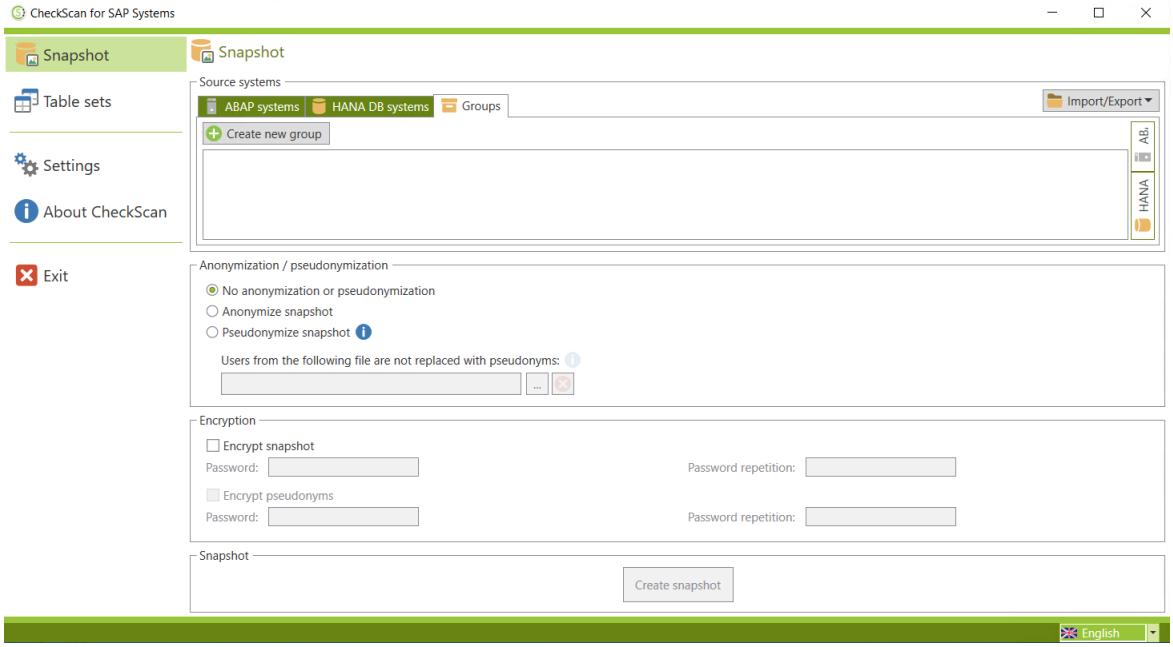



**Figure 27 - System connections in the group view**

You can use the Create new group button to create as many groups as required:

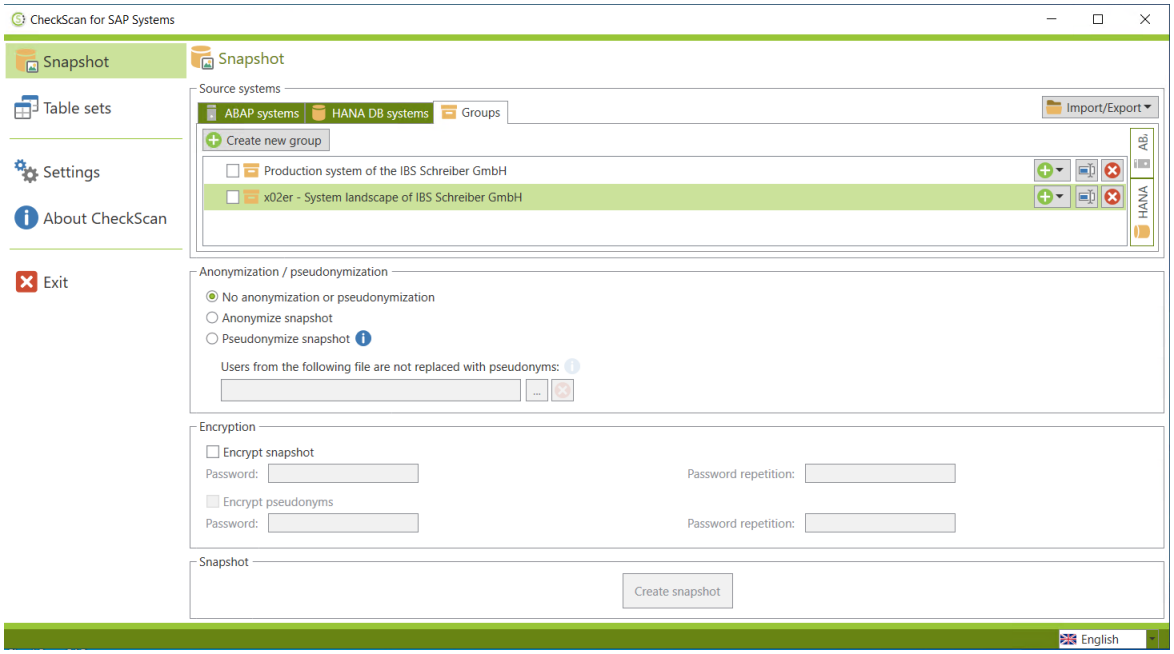



**Figure 28 - Created system groups**

The following buttons can be used to perform various actions on the groups:

 - Create a new system connection and add it to the group

 - Rename the group

 - Delete the group; the system connections linked to the group are not deleted in the process

You can use the *ABAP systems* or the *HANA DB* button to show a toolbox in which the previously created system connections are available for selection. You can use the button to display the toolbox permanently if necessary:

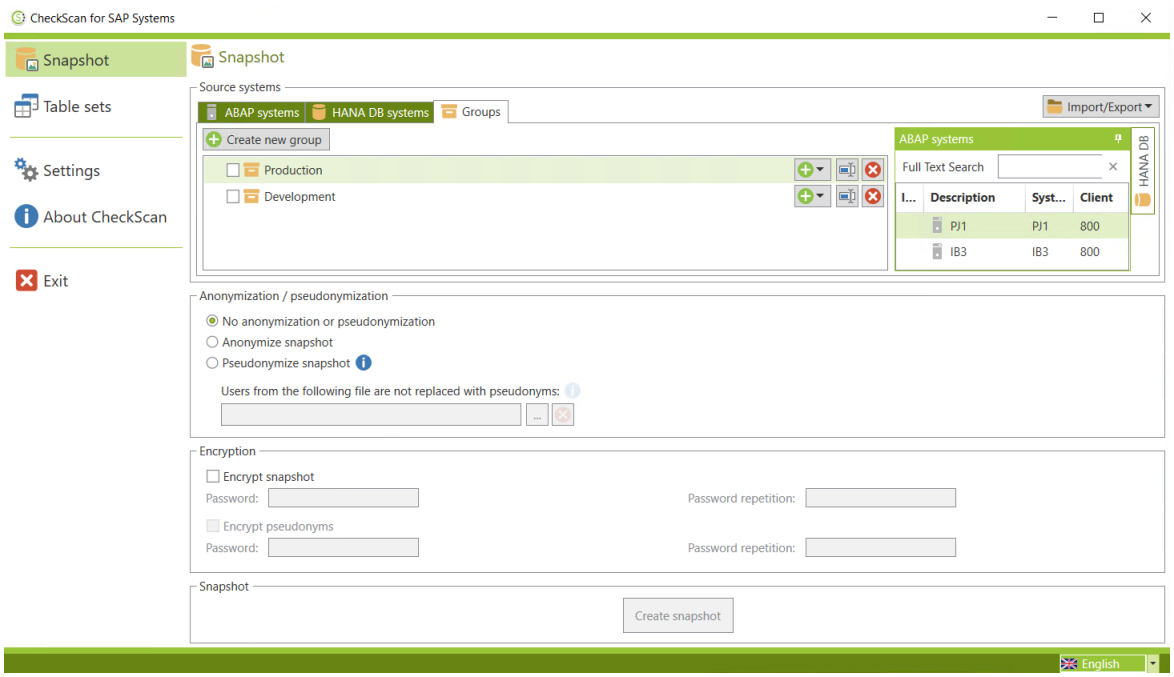



**Figure 29 - Group view including toolbox for selecting source systems**

The system connection can now be assigned to the groups required via drag&drop:

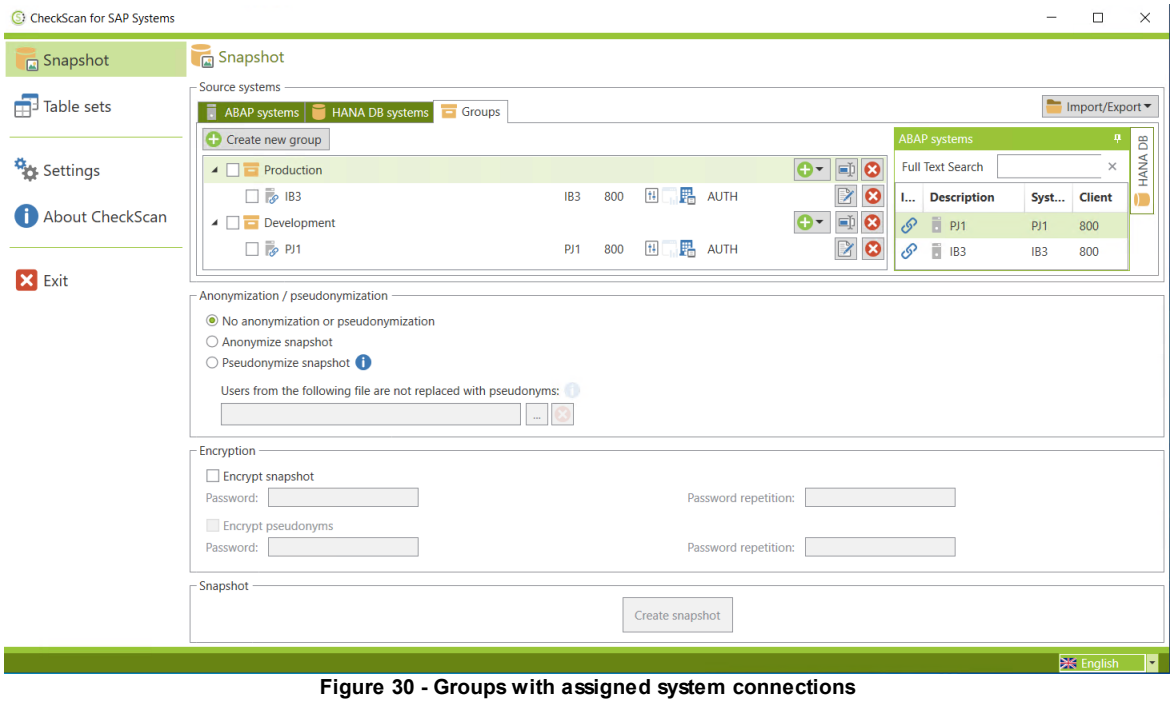



**Figure 30 - Groups with assigned system connections**

The icon in the toolbox with the system connections displays an active assignment to groups. The filter function can still be used to search the toolbox for specific systems among a large number of system connections.

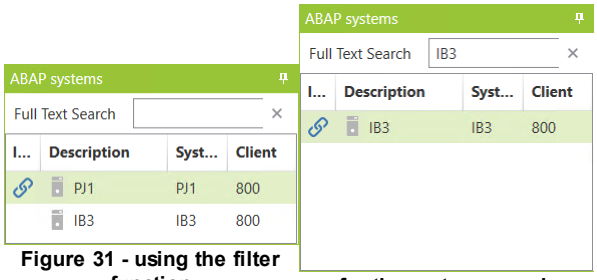



**Figure 31 - using the filter function for the system search**

## II - 9 Creating a snapshot (ABAP & HANA DB)

To create snapshots of the required SAP or HANA database source systems, one or more system connections must be marked with a flag in the list or group view:

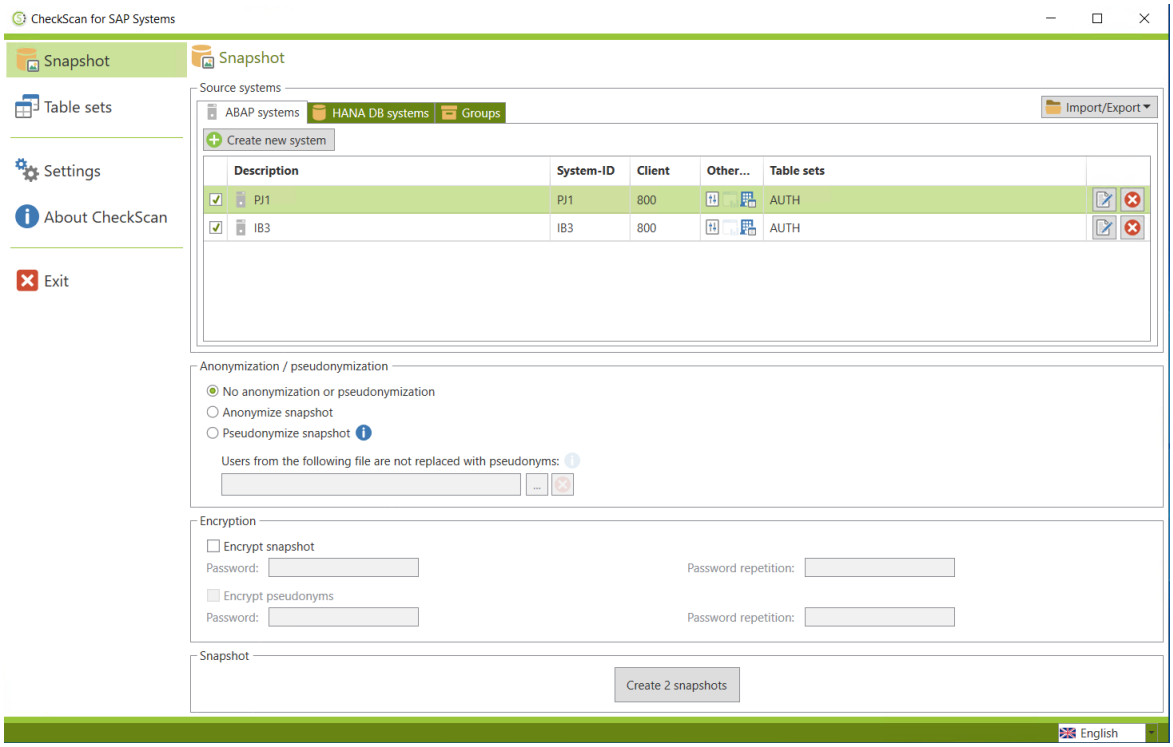



**Figure 32 - Systems marked for creating snapshots in the list view**

If several systems are marked for snapshots, the scan module reads them out sequentially and the relevant snapshots are saved in the target directory listed.

If necessary, the snapshots can also be encrypted using a password. This password is requested when the snapshot is imported to the evaluation module database.

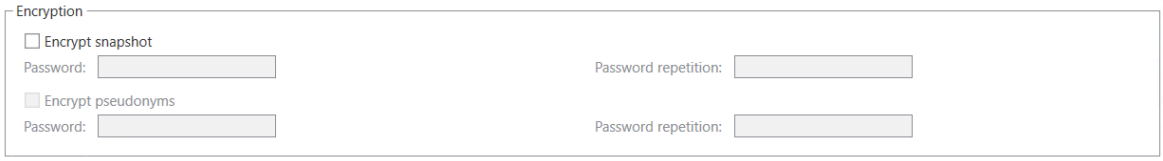



**Figure 33 - Optional snapshot encryption**

If necessary, the mapping file with pseudonyms to real names can be encrypted. This option is only available, when the snapshot will be pseudonymized and the option *Pseudonymize snapshot* is activated:

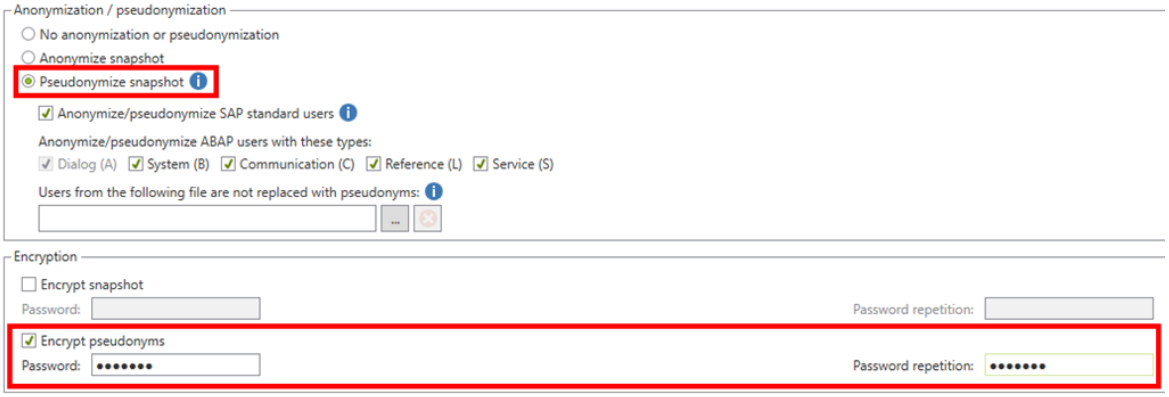
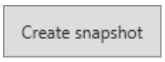



**Figure 34 - Optional encryption of mapping file**

Choose the 

button to create the snapshot. If there are no measures regarding personal data protection like scan via SNC, encryption of snapshots or pseudonymization, there will be a short warning regarding possible data protection violations:

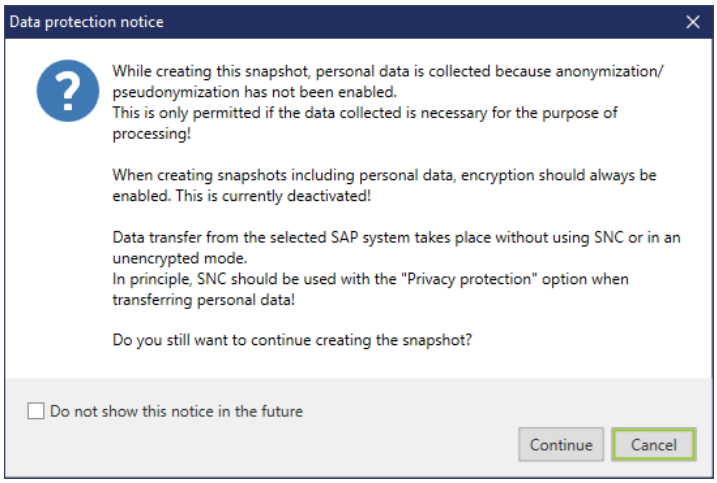



**Figure 35 - Warning regarding missing data protection measures**

Detailed information about safety measures during scan of personal data can be found in the separate CheckAud data protection guide.

In the next step, a dialog box for saving the snapshot file opens:

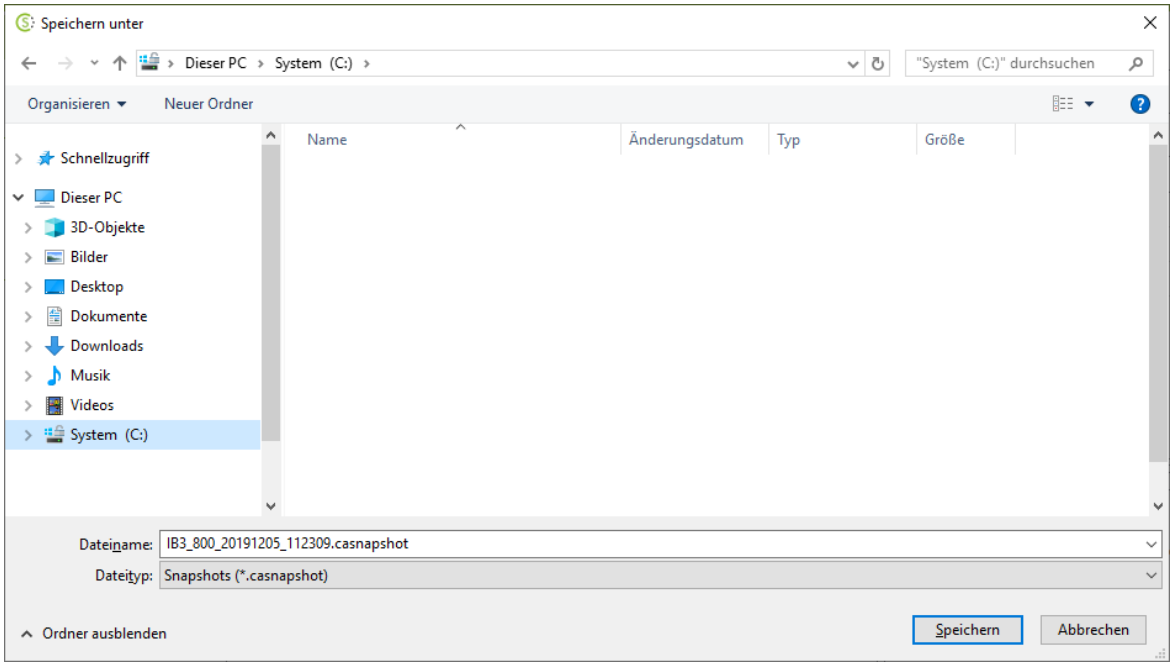



**Figure 36 - Standard Windows dialog window for saving the snapshot**

The name of the file to be saved is composed as follows:

*SystemID_Client_Date_Time.casnapshot*

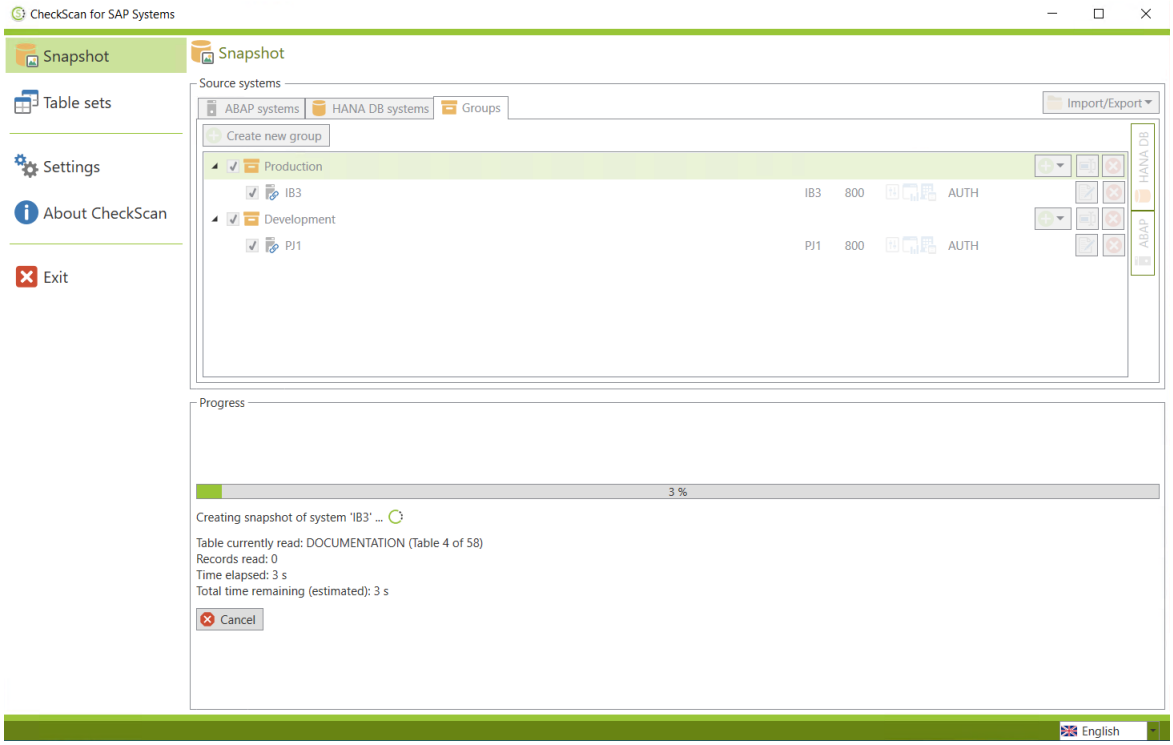



**Figure 37 - Scan progress**

After you start the scan, the system selection is deactivated and the lower area displays the tables to be scanned and the estimated time required to complete the scan. Once the scan is successfully completed, a results window is displayed:

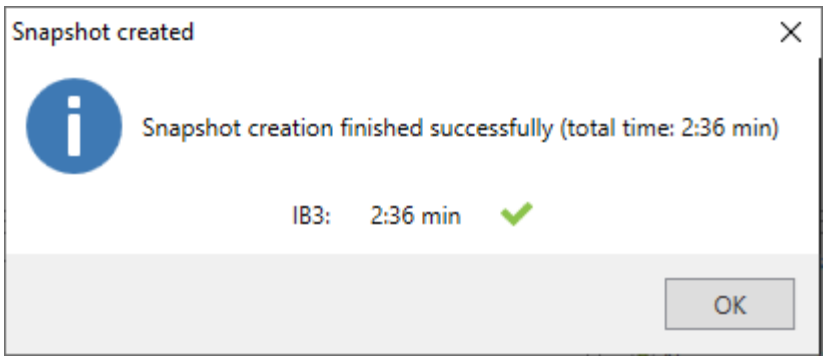



**Figure 38 - Results window for the successful scan**

**Note:**
A ⚠ icon in the results window indicates that some optional tables were not included in the snapshot. However, the snapshot was created successfully. If you place the mouse cursor on the icon that is displayed, a window appears that shows the tables that were skipped in the associated table set.

**Note:**
The procedure has to be done for ABAP-Scans and HANA DB-Scans seperately. With switching from Tab *ABAP Systems* to *HANA DB Systems* the scans can be started.

# Chapter III - CheckAud 2025.2 (Evaluation module)

# III CheckAud 2025.2 (Evaluation module)

## III - 1 User interface

The following figure shows the CheckAud 2025.2 user interface:

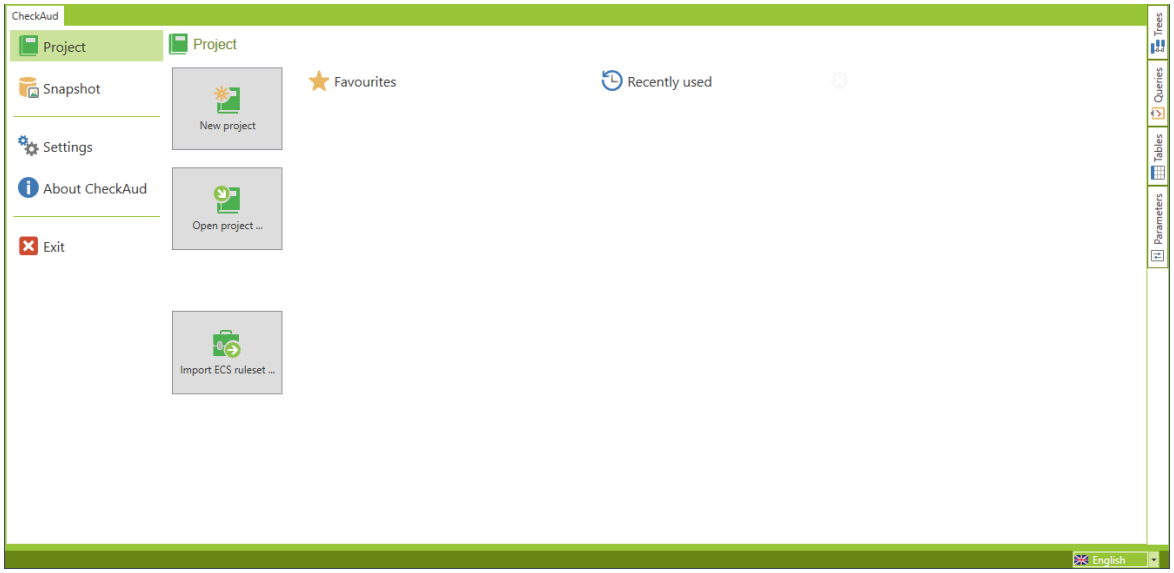



**Figure 39 - CheckAud start screen**

| | |
|---|---|
| *New project* | Project view for creating/editing analysis projects |
| *Open project* | Project view for analysis projects that have already been created |
| Import ECS ruleset | Import a ruleset from the Easy Content Solution (ECS) as a CheckAud analysis project |
| *Snapshot* | Import and manage snapshots |
| *Settings* | Global program settings |
| *About CheckAud* | Administrative license management and more detailed information about CheckAud |
| *Exit* | Closes CheckAud |

The project view displays the following additional user interface elements:

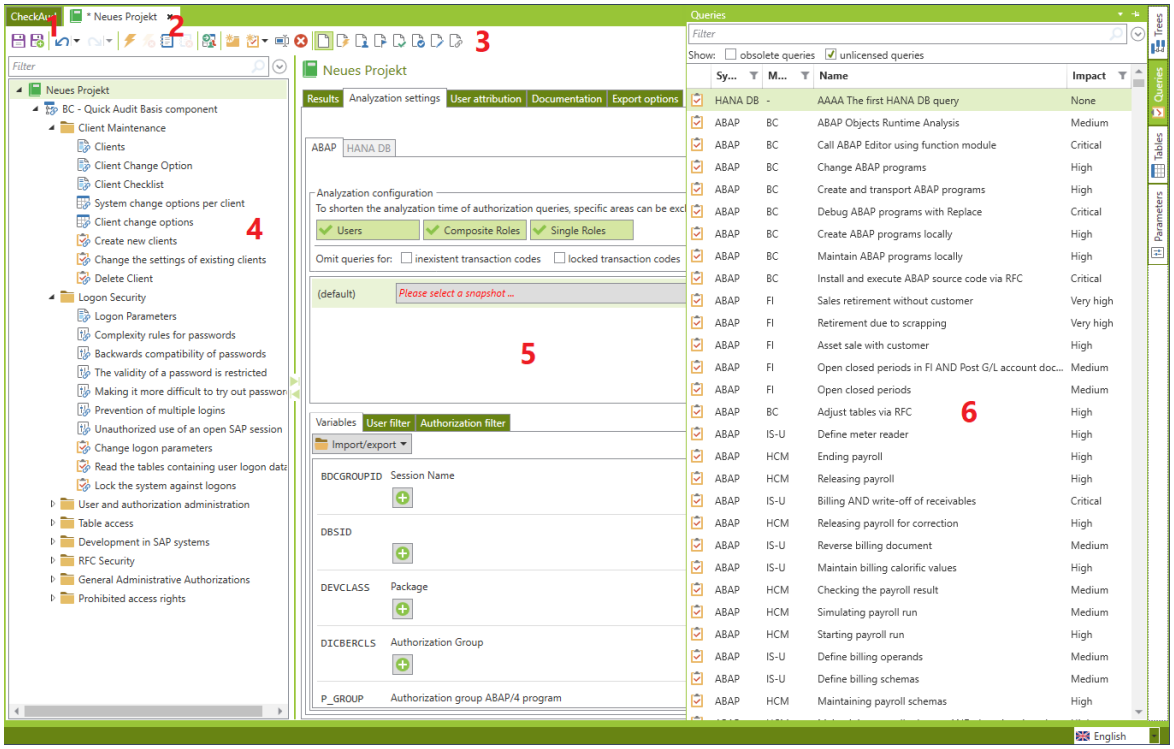



**Figure 40 - CheckAud project view**

*1* Switches to the start screen without closing the analysis project that is currently open.

*2* Tab for the current selected analysis project, every analysis project will be opend in own tab so several projects can be opened at a time

*3* Quick access menu for standard functions

- Save project
- Save project as
- Undo
- Redo
- Start analysis (project, subproject or current selected query)
- Cancel analysis (project, subproject or current selected query)
- Export the results for the selected element in the analysis project
- Cancel the results export
- Create a new directory in the analysis project
- Create a new ABAP or HANA DB query in the analysis project
- Rename the current selected element in the analysis project
- Delete the current selected element in the analysis project

- Show the standard project tree view
- Display the inheritance of the analysis settings in the project tree view
- Display the inheritance of the user assignment in the project tree view
- visualize changes in impact of authorization queries
- visualize the definition of mitigation controls of authorization queries
- visualize changes in assessment criterias of tabular queries
- visualize changes in documentation of authorization queries
- visualize not referenced elements in the project

*4* Analysis project, this displays the current selected analysis project in a tree view. Changes to the project structure are made here.

*5* Main window, *i*n this area, you configure content-related project settings such as the settings for the SAP scan used, filter or variable settings and settings for risk evaluations for individual queries in the project.

*6* Toolbox, this toolbox provides all the authorization queries, table queries and parameter queries predefined by IBS. On the Trees (Bäume) tab, the supplied queries are sorted by theme in the form of templates. The toolbox is hidden by default but can also be permanently displayed by clicking 

*7* Language selection, *y*ou can use this button to switch between the specified languages (the defaults are German and English). When you do so, both the user interface and the contents of the projects switch to the new language setting.[1]

[1] If translations have been maintained for the language selected in the project

## III - 1.1 Project - New Project / Open Project

In this menu item, you can create new analysis projects or open existing ones. You can also open the last used projects with quick access. After projects are opened or saved, they are stored in chronological order in the *Recently used* area. If necessary, click the  button to add individual projects to the favorites list. Projects that are marked as favorites can be removed from the favorites list by pressing the  button again.

The  and.  buttons allow you to change the sort order in the favorites list.

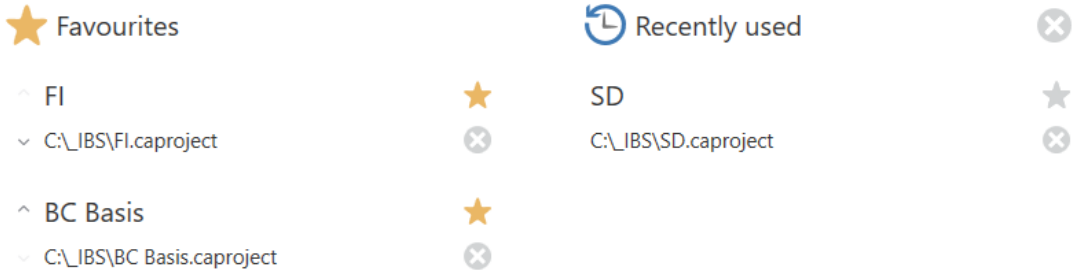



**Figure 41 - Last analysis projects used**

Click the button to remove the last opened analysis projects or favorites from the lists.

## III - 1.2 Snapshots

The *Snapshot* menu item lets you import snapshot files created by the CheckScan scan module. You can also manage already imported snapshots.

### III - 1.2.1 Importing snapshots

To import the snapshot files created by the scan module, proceed as follows. From the *Snapshot* menu item, start the import of a snapshot created by CheckScan using the button *Import snapshot*:

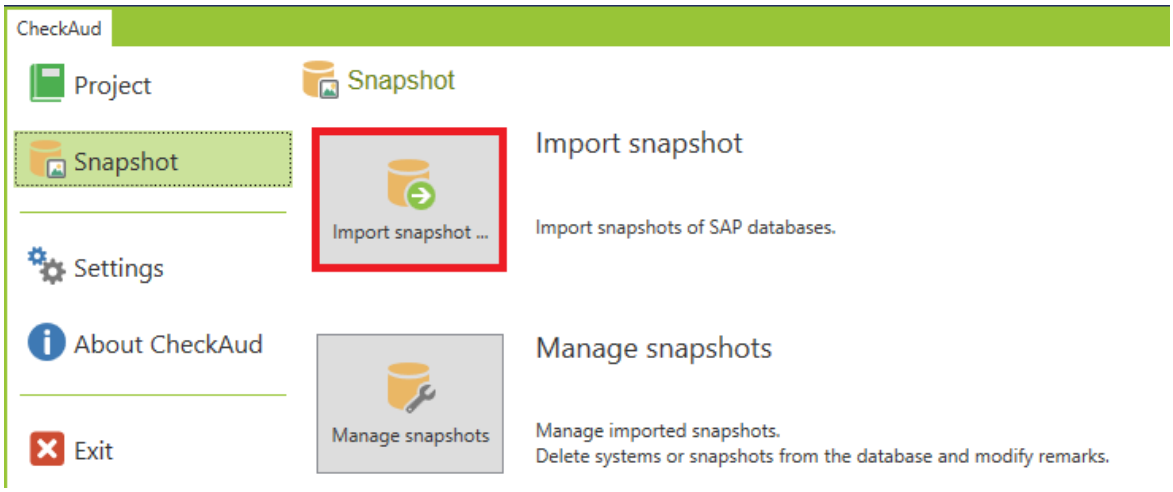



**Figure 42 - Importing snapshots**

A standard Windows dialog box for selecting files opens. Here, you have to select a snapshot file that has already been created. You then import the file:

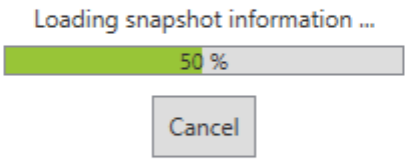



**Figure 43 - Importing the snapshot file**

Before the actual import, the initial information about the imported snapshots is displayed in an overview:

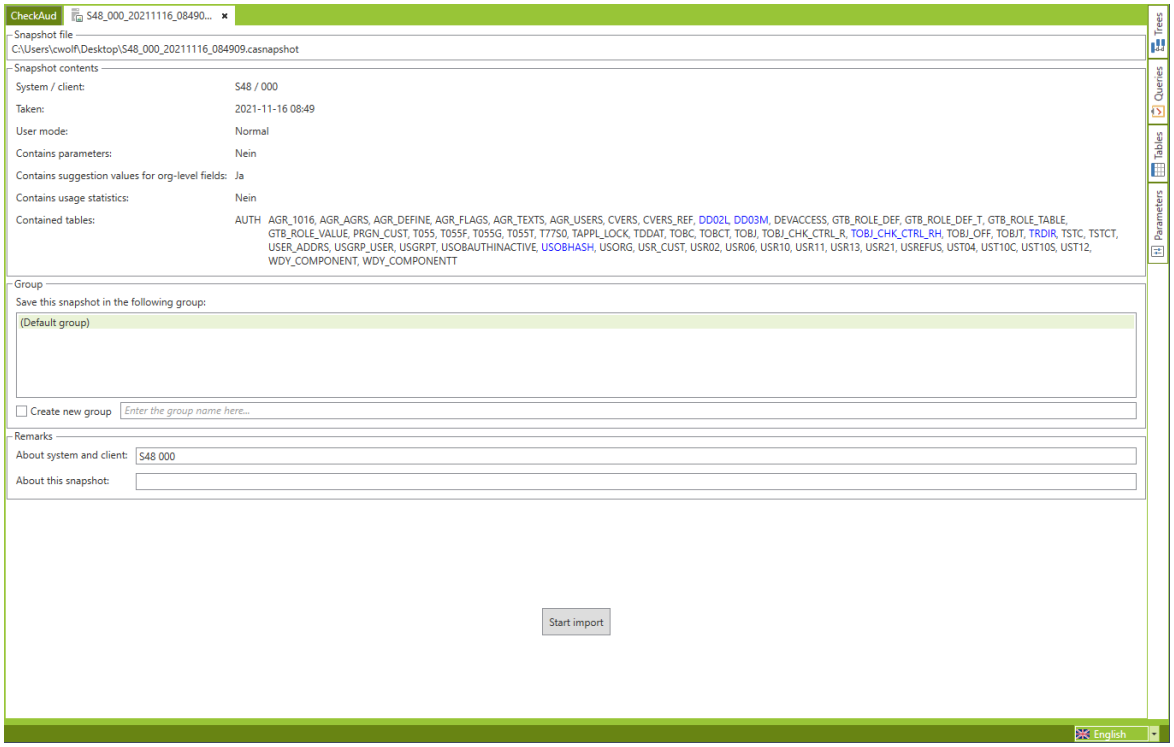



**Figure 44 - Import dashboard ABAP**

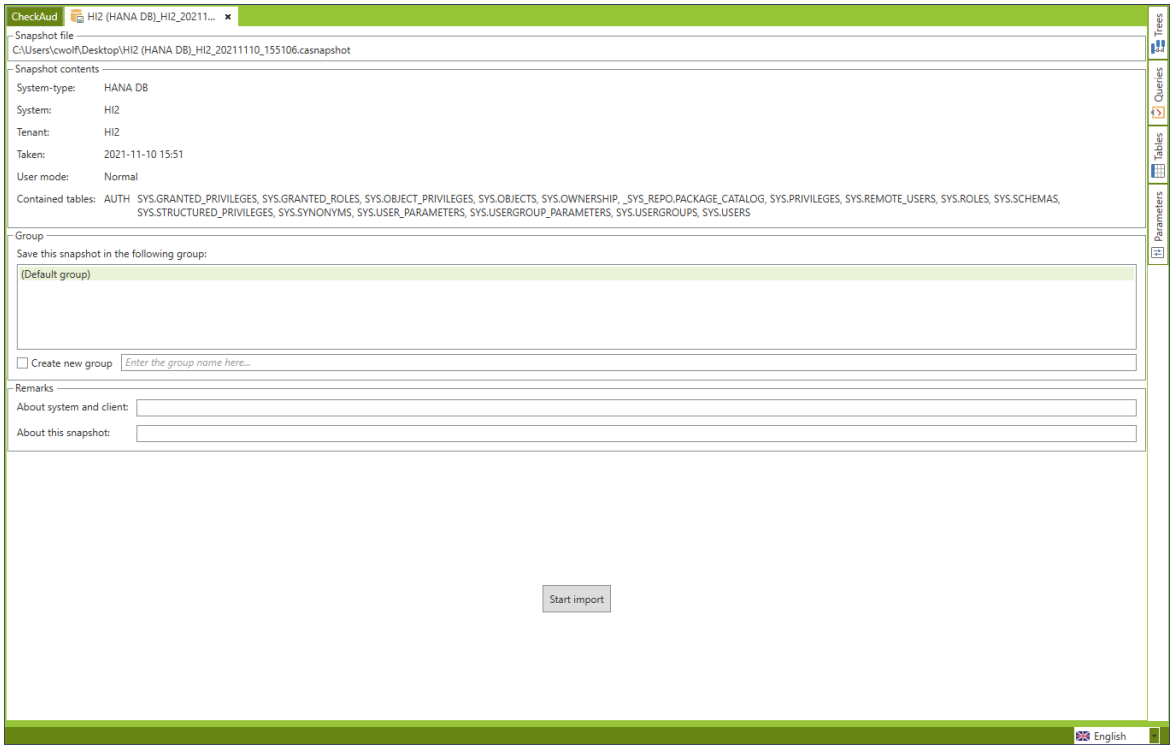



**Figure 45 - Import dashboard HANA**

The information includes:

- System/client (ABAP snapshot) or system / tenant (HANA DB snapshot)
- The snapshot creation date
- The user mode (normal, anonymized or pseudonymized)
- Whether parameter values have been read out
- Whether default values for org levels have been read out
- The table sets stored in the snapshots

Furthermore the new snapshot can be assigned to a snapshot group. Group assignment is a good way to optimize the snapshot management. Instead of using the default group, snapshots can be assigned in own groups (in case these groups are created in the snapshot management). It's also possible to create a new group during the import process.

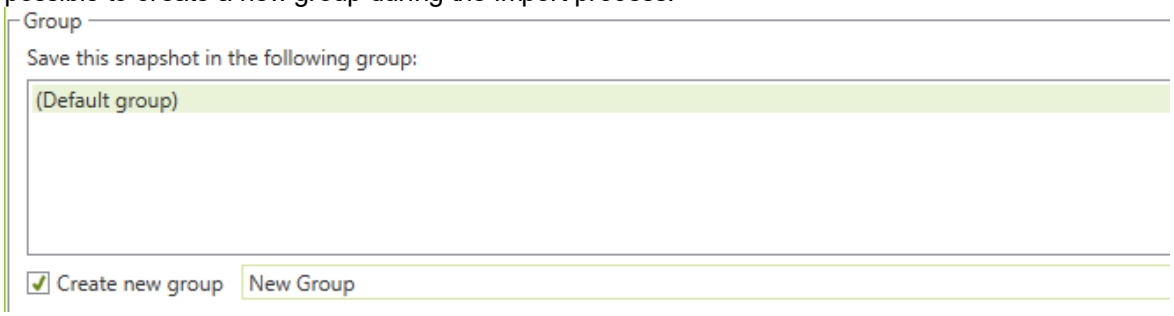



**Figure 46 - Group assignment**

Optional comments about the clients or snapshots can also be stored with this information. All the information displayed (and maintained, if necessary) here is also subsequently displayed in the Administration area for the snapshots

You can choose Start import to start the import and the preparation of the snapshot data in the CheckAud database:

**Note:** Some table names may be highlighted in color in the included tables area:

| | |
|---|---|
| **Black** | Tables that have been fully read out |
| **Blue** | Tables that have not been fully read out due to a filter criterion; the filter criterion in question is displayed when you move the mouse over the table name |
| **Red** | Tables that were specified in the configuration of the table set used for the scan but that could not be read out. The reason for this may be that the tables are unavailable in the SAP system or that the RFC interface user/scan user did not have the authorization to read out these tables. |
| **Grey** | Tables that were skipped during the readout because anonymization or pseudonymization was enabled during the scan and some of the contents of these tables are therefore unavailable for the evaluation. |

### III - 1.2.2 Manage available snapshots

Choose *Snapshot* and *Manage snapshots* to manage the snapshots that have been imported to CheckAud.

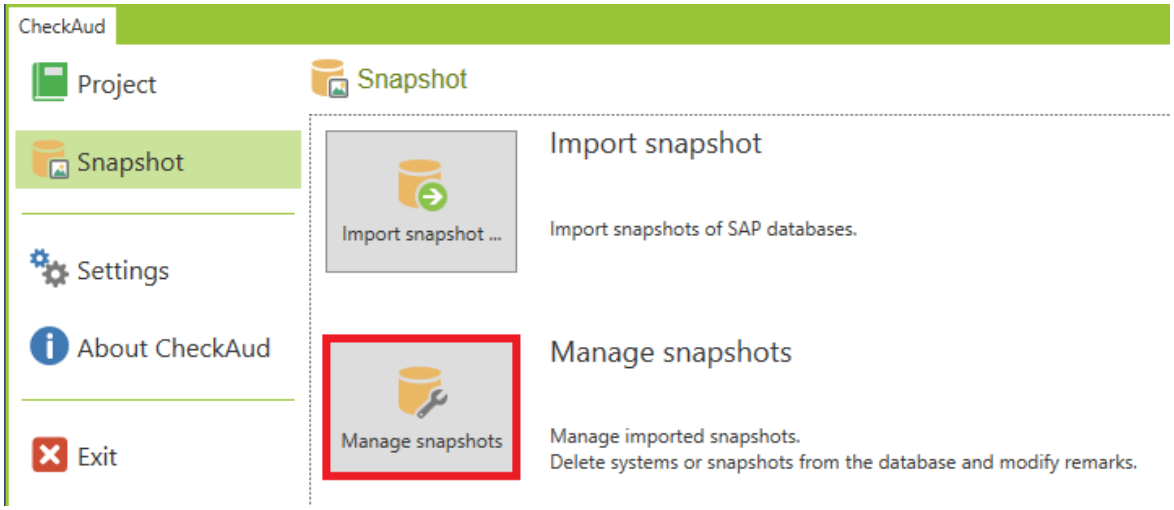



**Figure 47 - Administration start screen for snapshots**

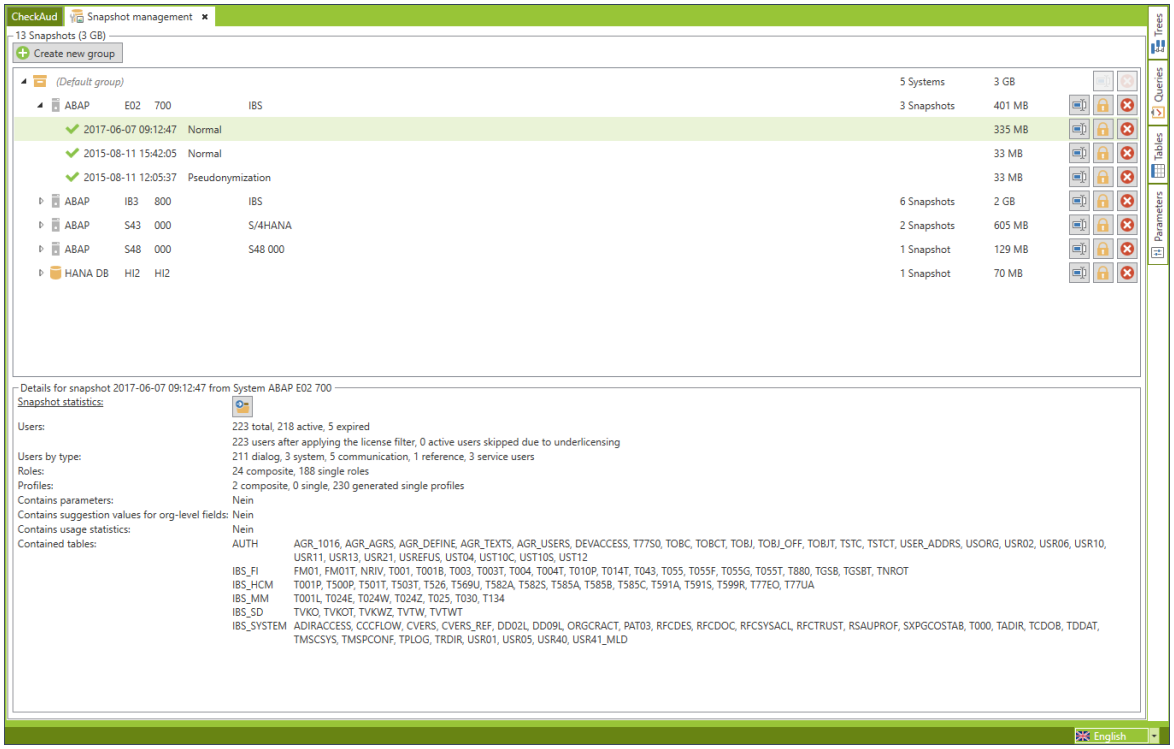



**Figure 48 - Snapshot Management**

*Snapshot Management* provides information about the snapshots that are available in the CheckAud database. These snapshots are displayed in a table sorted by group, type of snapshot (ABAP or HANA DB) system, client or tenant. Multiple buttons and information icons are provided to help you manage the snapshots

| | |
|---|---|
|  | The imported snapshot for the system/client is licensed and can be used |
|  | Change a comment about the system/client and/or snapshot |
|  | Protect the system/client and/or snapshot from being deleted from the database |
|  | Delete the system/client and/or snapshot |
|  | Display statistical information about the snapshot |
|  | Export the snapshot statistics to a text file |
|  | The number of SAP users in the snapshot is covered by the CheckAud license used; there are no license violations |
|  | The number of SAP users in the snapshot is not covered by the license used; there is a license violation or the snapshot was created with other license settings. In this case, you should contact IBS Schreiber GmbH Support. |

The snapshots of the CheckAud database can be organized with *groups*. The *default group* contains every single snapshot as long as these snapshots are not assigned to a new group during the import process.

With the button 

new groups can be created. Snapshots will be assigned to these new groups with Drag&Drop. Within this group, the snapshots will be automatically also grouped by system, client / tenant.

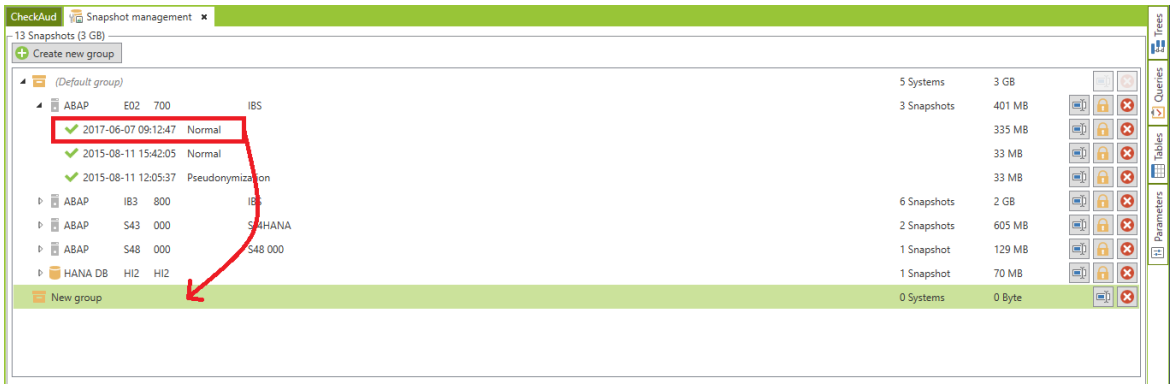



**Figure 49 - Creation of snapshot group and assignment of snapshotSnapshots**

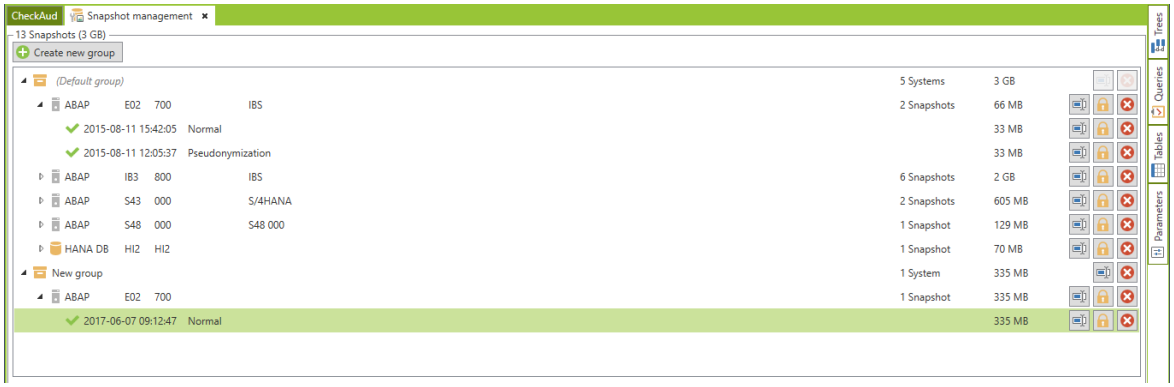



**Figure 50 - New snapshot group**

Later this group can be used in the analyzation settings of the analysis project:

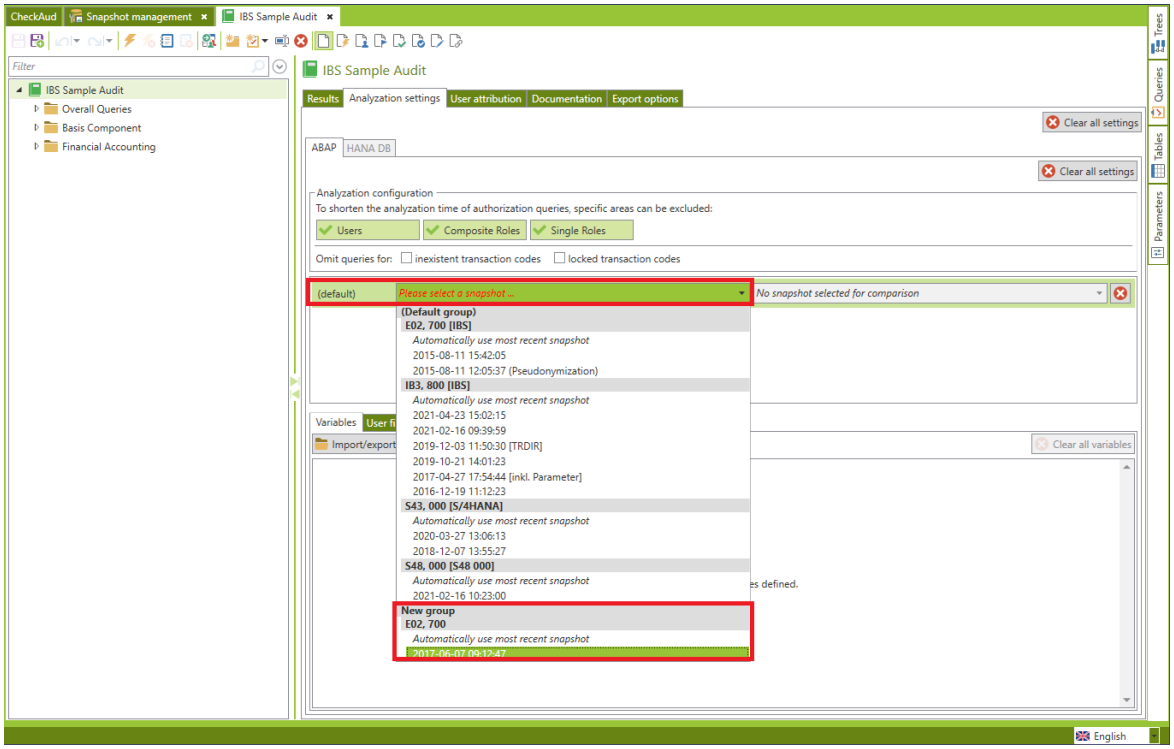



**Figure 51 - Usage of snapshot groups in analyzation settings**

## III - 1.3 Settings - Default language / Server / Export settings

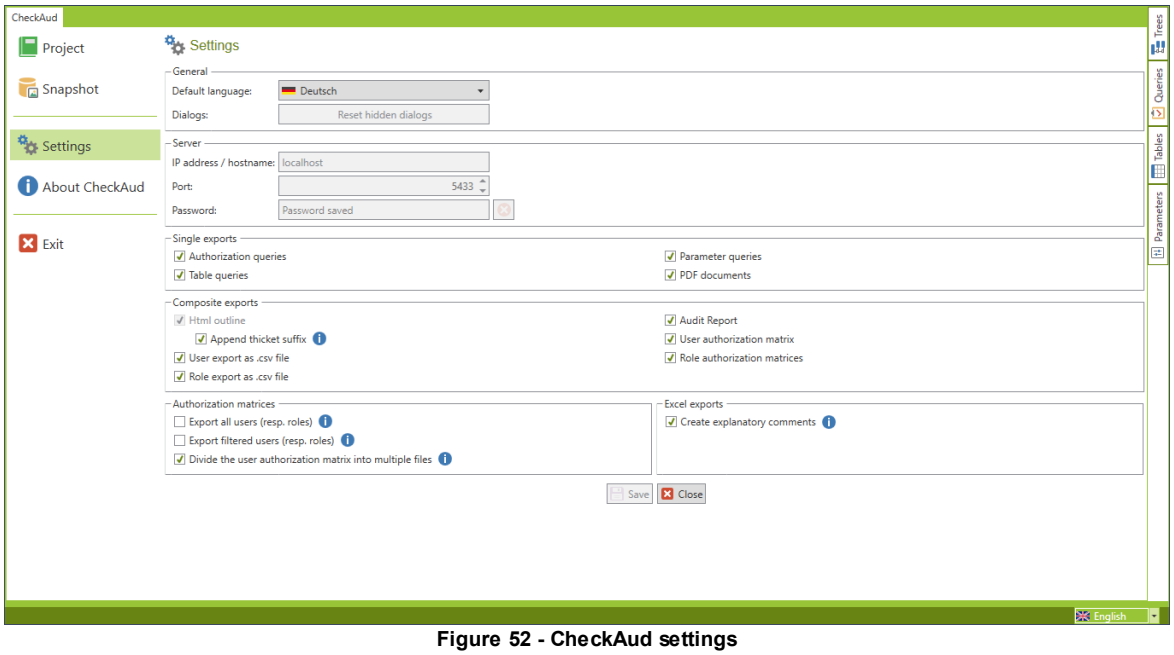



**Figure 52 - CheckAud settings**

*Default language :*

CheckAud can be used in several languages. The standard program functions and the contents of the analysis projects supplied with the standard system are available in both German and English. You change the language using the Deutsch and English buttons.

Depending on the configuration, CheckAud always starts in this selected language but the language can be changed at any time during operation.

*Dialogs:*
Some Dialogs can be hidden with the option *Do not show again,* with this button, hidden dialogs will be shown again.

*Server:*

This display the server address and port settings configured during the installation. You cannot change these settings.

*Single exports, Composite exports, Authorization matrices, Excel exports:*

The settings configured here for exporting evaluated analysis projects here apply throughout the program. When you create a new analysis project, the settings are automatically applied to the project as default settings. You can configure these settings differently from the global program defaults in the respective analysis projects. For more information, see the chapter Settings 153 partial/full exports.

## III - 1.4 Docking tabs and toolboxes

You can dock tabs and toolboxes to customize your user interface. You can position tabs and toolboxes anywhere on the screen as separate windows using drag and drop. To do so, you simply click and hold the mouse button on the desired tab or toolbox to move it from its current position to the screen area of your choice:

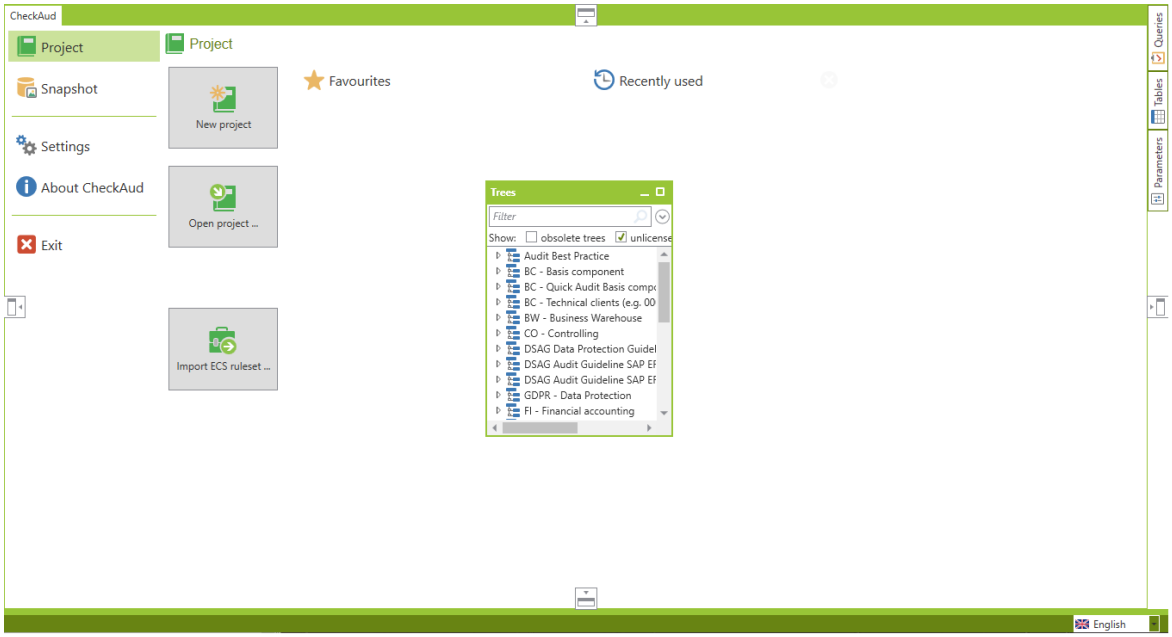



**Figure 53 - Docking tabs and toolboxes**

You can also do this with the tabs of open analysis projects. The project tabs can be disconnected from the main window and moved on the screen.

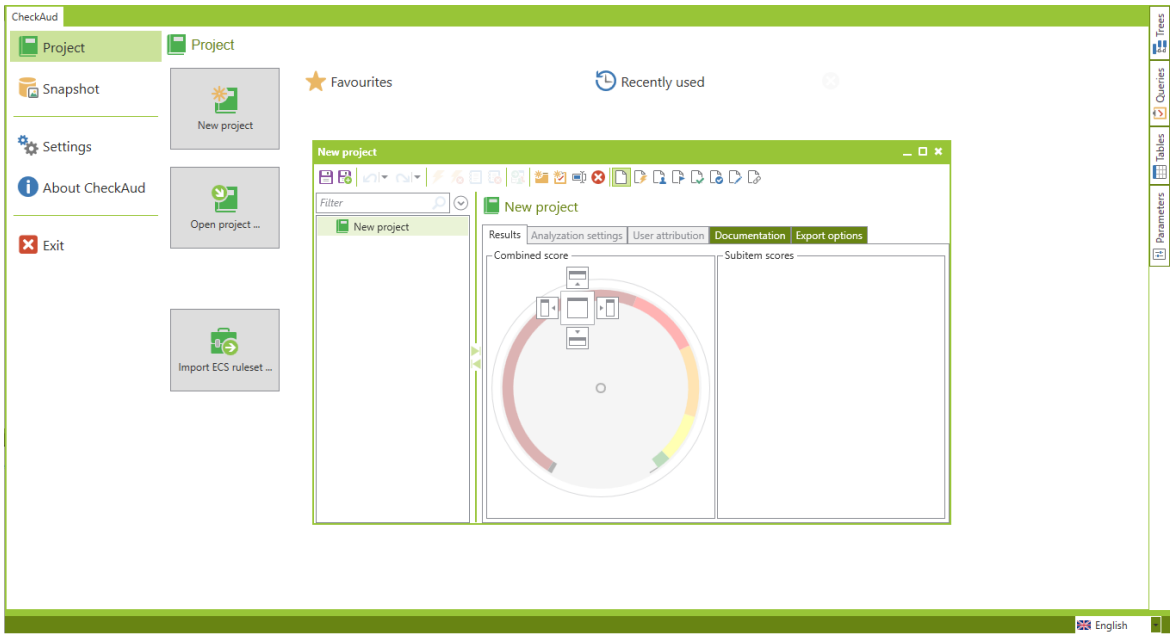



**Figure 54 - Docking analysis project tabs**

A navigation cross is provided as an additional aid that is displayed automatically when you release a tab or toolbox as a window using drag and drop. You can determine the position of the new window using the navigation cross.

**Figure 55 - Docking navigation cross**

The outer points of the navigation cross stand for top, bottom, left and right. The center point restores the standard view. Alternatively, you can also restore the default view using the *Restore default layout* menu item that is displayed when you left-click the title bar of a window. When you close CheckAud, the customized interface layout is saved. This ensures that the layout is retained the next time that you start CheckAud.

## III - 1.5 Working with the clipboard

You can copy the contents of the analysis project or the information listed in the table views to other programs using the clipboard. Right-click in the result window of an authorization query, for example, to open the context menu. You can copy either a single cell or the entire row. When you choose *Copy*, the other cell values are also displayed. You can individually select and copy them as required.

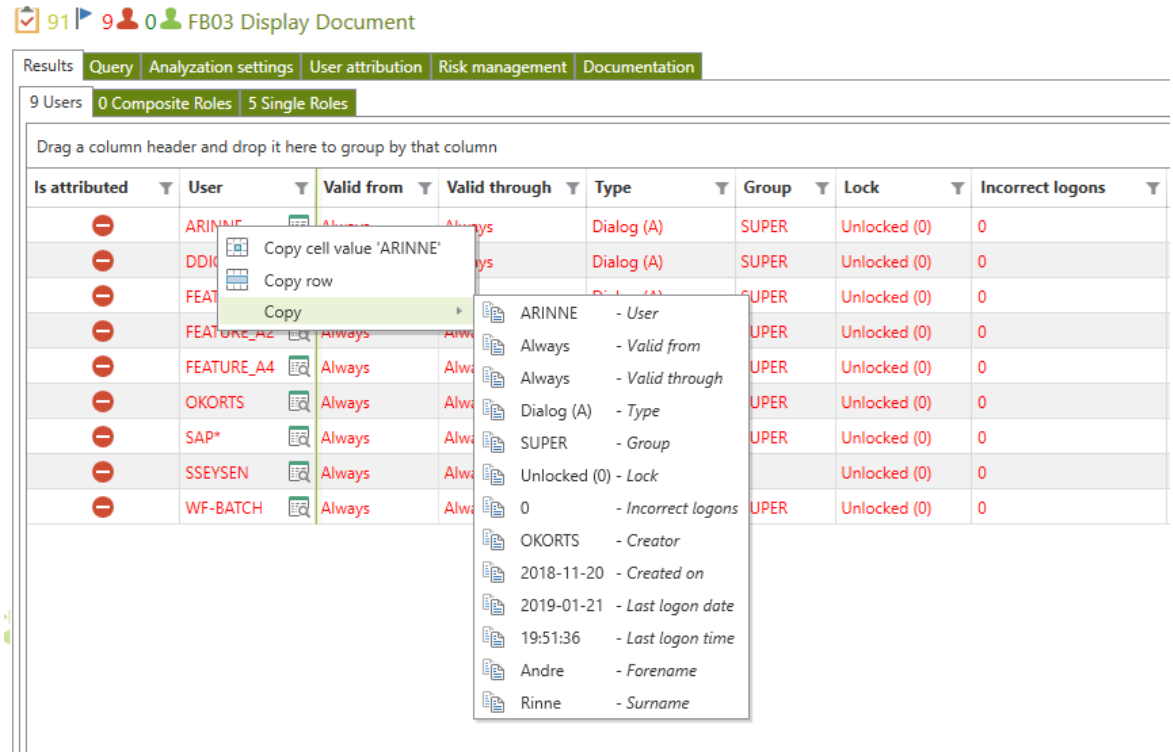



**Figure 56 - Copying values**

You can copy the text content of the elements in the analysis project using the clipboard. In the example below, the copied value is FB03 - Display document.

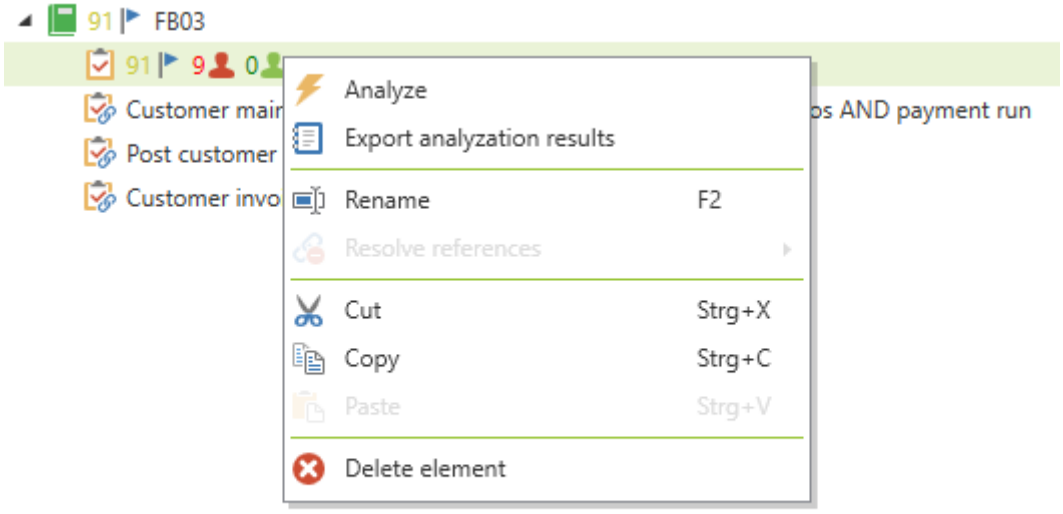



**Figure 57 - Copying element content**

# III - 2 Analysis projects

## III - 2.1 Introduction

Analysis projects contain technical queries and all the settings, specifications and information for performing a check. The structure of the analysis project can also reflect the procedure for performing the check. In addition, you can define the following settings/information for an analysis project:

- The snapshots to be evaluated (= snapshots of the applicable SAP systems or HANA DB databases): You can use multiple snapshots of different systems and clients in one project.
- Filters: You can include or exclude specific user accounts in the evaluation. Extensive selection criteria is provided, including user attributes (status, valid until, namespace), roles and profiles.
- Variables: You can define specifications for queries with variables in the analysis projects (queries that reference org. levels such as company codes and business areas, for instance).
- User assignment: You can define individual target specifications regarding authorized users for each query. These specifications have a neutral effect on the calculated query score (see the chapter The Analysis Project Score 177)
- Risk management settings: The assessments for the risks behind the technical query are defined here. You also define technical descriptions of the risk, information about the potential damage and organizational controls that can compensate for the effects the damage.

- Documentation: You can enter keywords (tags) for searches within the project here. You can also maintain more detailed information about the area of application and objectives of the technical authorization query.

Double-click previously created analysis projects from Windows Explorer to open them directly with CheckAud. The project files are identifiable by the file extension *.caproject and* the  icon.

## III - 2.2 The elements of an analysis project

 Project

The starting point for each analysis is the analysis project. The settings configured for the analysis at this level are inherited to all its subelements. The element can be given any name in German or English. You can expand or collapse all the project subitems by pressing and holding the Ctrl key and clicking the arrow to the left of the project icon.

 Folders

Folders constitute the organizational containers within the project. A folder can inherit settings or be assigned with new analysis settings by interrupting the inheritance. These new settings are then inherited to its subelements. The element can be given any name in German or English. You can expand or collapse all the folder subitems by pressing and holding the Ctrl key and clicking the arrow to the left of the folder icon.

 Authorization query

The authorization query is the technical check of (fully customizable) combinations of authorization objects that a user may receive due to his or her assigned roles, profiles or reference users. This authorization query generally covers a risk that can be quantified by the check, including the assessment defined in the authorization query. The element can be given any name in German or English.

 Authorization query (reference)

This authorization query is a standard IBS authorization query whose technical composition and name cannot be changed. Custom settings can be configured only for the information about the effect of the damage, a description of the risk and the user assignment. Reference queries are automatically updated where necessary by updates in the configuration.

 Analysis tree (reference)

IBS provides theme-related configurations of standard queries based on best practice experience in the form of analysis trees. You can expand or collapse all the analysis tree subitems by pressing and holding the Ctrl key and clicking the arrow to the left of the analysis tree icon. You can integrated these analysis trees into your own analysis project as references. When you do so, you cannot change the structure or name of the queries included in the referenced analysis tree. Like in the reference queries, you can only define specific information about the effect of the damage, a description of the risk and information about the user assignment here. Referenced analysis trees are automatically updated where necessary by updates in the structure and composition of the included queries.

 Documents (reference)

This is the documentation stored in the analysis trees. It includes not only explanations of individual parameters and technical terms, but also information from our best practice experience. These documents are provided by IBS Schreiber GmbH and cannot be changed.

 Table query (reference)

These queries are predefined table queries provided by IBS Schreiber GmbH. A table query consists of a JOIN of one or more SAP tables or HANA database tables that have been read out with the snapshot based on the table set. You can also define filters for table content and specifications for the evaluation. You cannot change the composition of and the tables selected in a referenced table query.

 Table query

This is a table query that you have created yourself. You can use any SAP tables or HANA database tables included in the snapshot for any JOIN operations and filters here.

 Parameter query

This is a check of one or more SAP system parameters. If the parameters are provided with the snapshot (see the Parameters chapter), you can check the parameters against specific target specifications.

[1]Unless the folder is an element in a reference analysis tree that has been incorporated into your own analysis project.

## III - 2.3 Analysis settings

The Analysis settings tab contains the settings that apply to the overall project or to the selected element in the analysis project. There are different settings for ABAP and HANA DB systems.

- The authorization evaluation level
  - ABAP users, composite roles, individual roles
  - HANA DB users, roles
- The snapshot to be evaluated or compared
- The variables to be used (definition of organizational levels, only ABAP)
- The user filters to be used (which users are or are not to be displayed in the results)
- The authorization filters to be used (taking the sources of the authorizations into account during the evaluation)

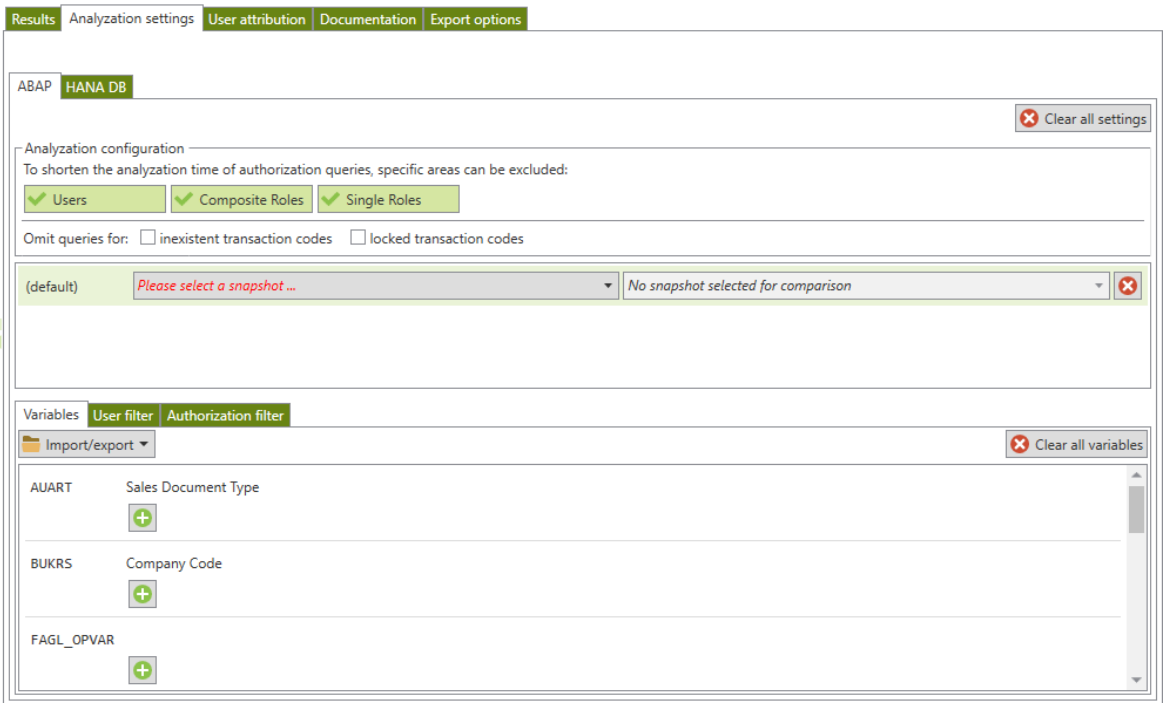



**Figure 58 - Analysis settings (ABAP)**

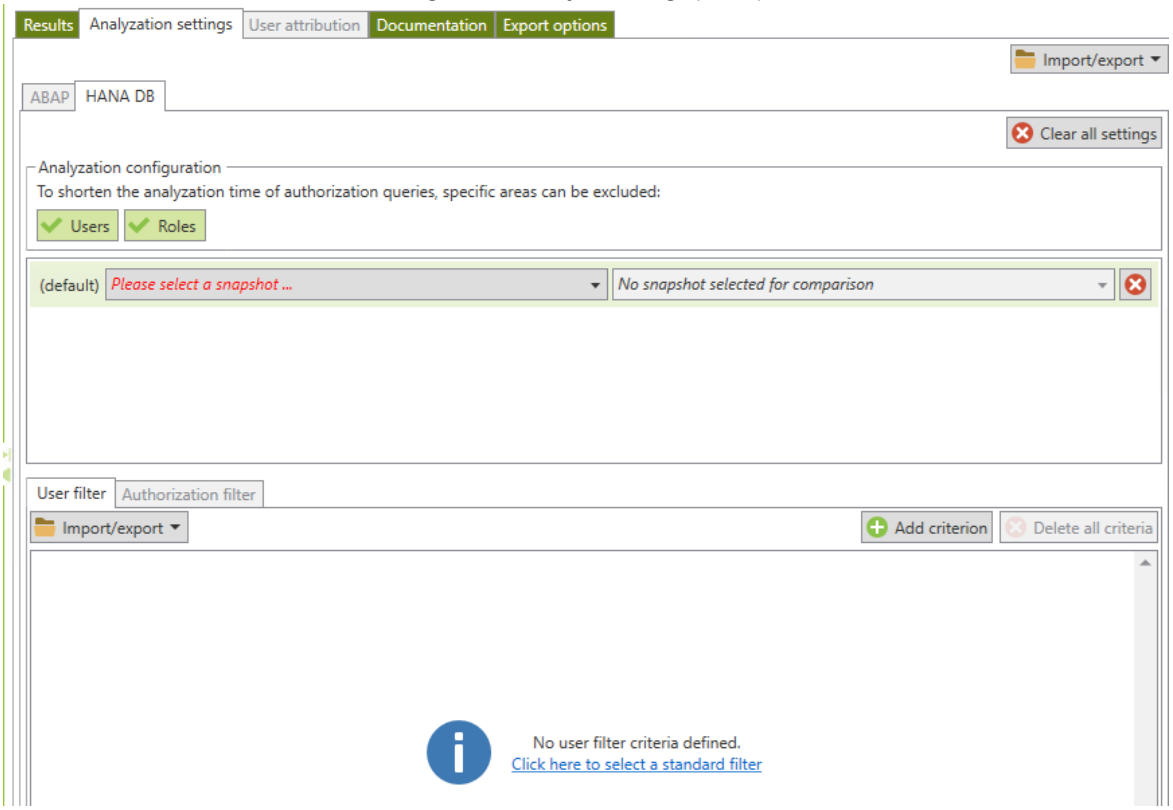



**Figure 59 - Analysis settings (HANA DB)**

### III - 2.3.1 Authorization evaluation level (ABAP)

Authorization queries can be evaluated on different levels:

| | |
|---|---|
| Users | The application evaluates all users that receive the authorization under inspection based on the individual roles, composite roles, profiles and reference users assigned to them. |
| Composite roles | All composite roles that fully include the authorization under inspection are evaluated. The sources of the authorization levels from the composite roles are also taken into account in this case. |
| Individual roles | All individual roles that fully include the authorization under inspection are evaluated. |

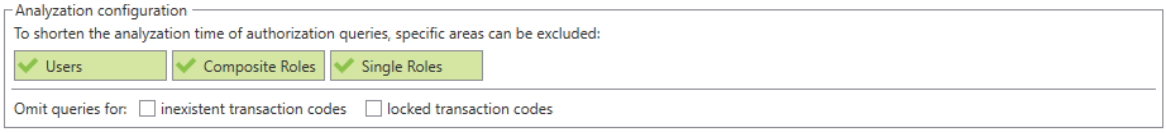



**Figure 60 - Evaluation levels**

You can choose which authorization evaluation level you want to activate using the *Users*, *Composite Roles* and *Single Roles* buttons. For example, if evaluations of composite or individual roles are not required, you can disable them and therefore improve the runtime of the evaluation:

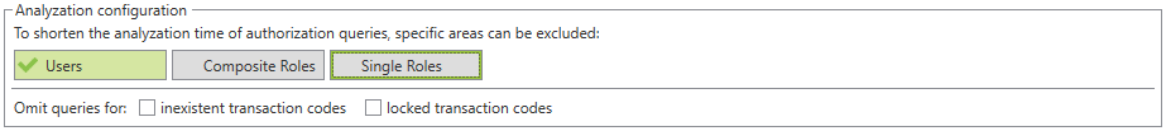



**Figure 61 - Selected evaluation levels**

### III - 2.3.2 Authorization evaluation level (HANA DB)

Authorization queries can be evaluated on different levels:

| | |
|---|---|
| Users | The application evaluates all users that receive the authorization under inspection based on the roles assigned to them. |
| Roles | All roles that fully include the authorization under inspection are evaluated. |

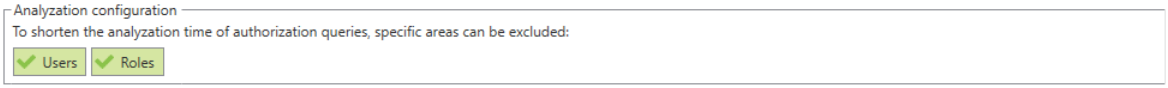



**Figure 62 - Evaluation levels**

You can choose which authorization evaluation level you want to activate using the *Users* or *Roles* buttons. For example, if evaluations of roles are not required, you can disable them and therefore improve the runtime of the evaluation:

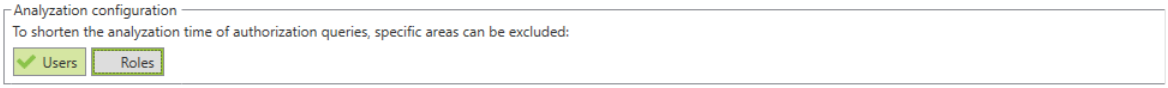



**Figure 63 - Selected evaluation levels**

### III - 2.3.3 Considering non existing or locked transactions

An authorization query usually contains all relevant transactions, wether these are useable in the SAP system or not. For example, the transaktion SE16N doesn't exist in a business warehouse SAP system.

During the setup of an SAP authorization concept, some of these transactions will be included in roles generally, because (in this example) the roles from an ERP system will be used in the BW system with only minor changes. Therefore it is possible, that roles in the BW system will have transactions, which the BW system doesn't provide. Although the roles provide access rights for these transactions, it is not possible to use these transactions and therefore the assignement of these "not known" transactions in roles won't have any effect.

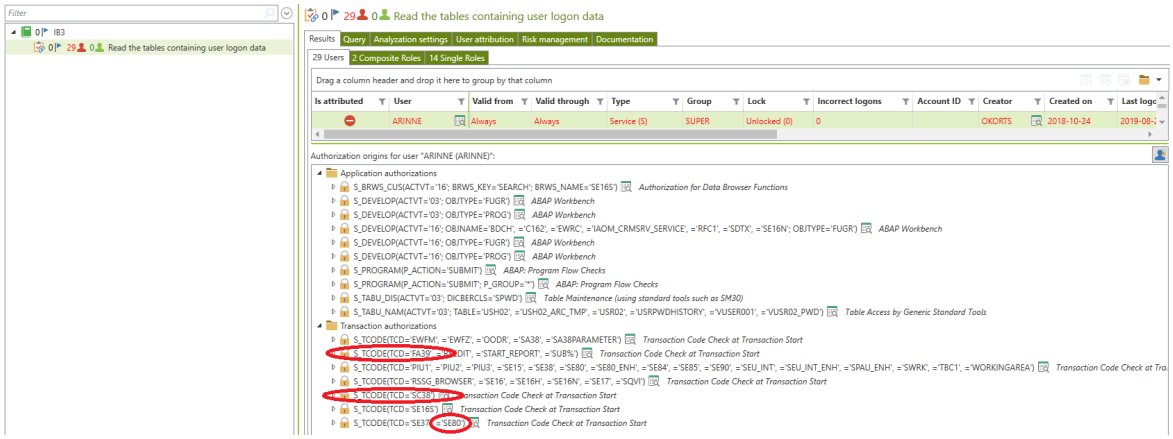



**Figure 64 - Result with all checked transactions**

To minimize false positives, it is possible to configure CheckAud not to consider non existing transactions. In the tab *Analyzation settings* you can activate the flag *inexisting transaction codes* to reduce the evaluation of authorization queries down to only existing transactions applicable for the actual SAP system.

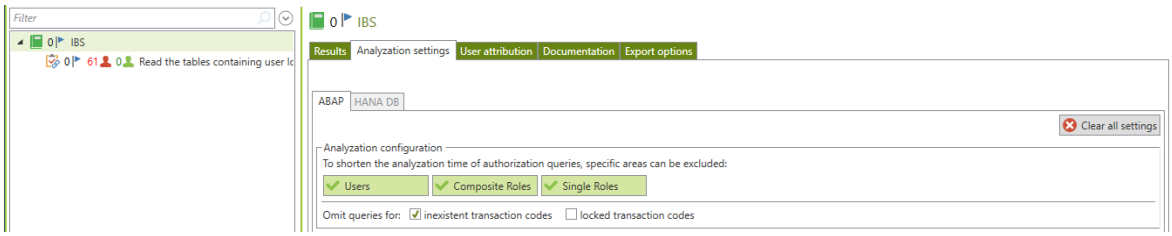



**Figure 65 - activate flag inxistent transaction codes**

In comparison with the first evaluation above, you can realize, that the transactions FA39 and SC38 ar not listet in the authorization origin:

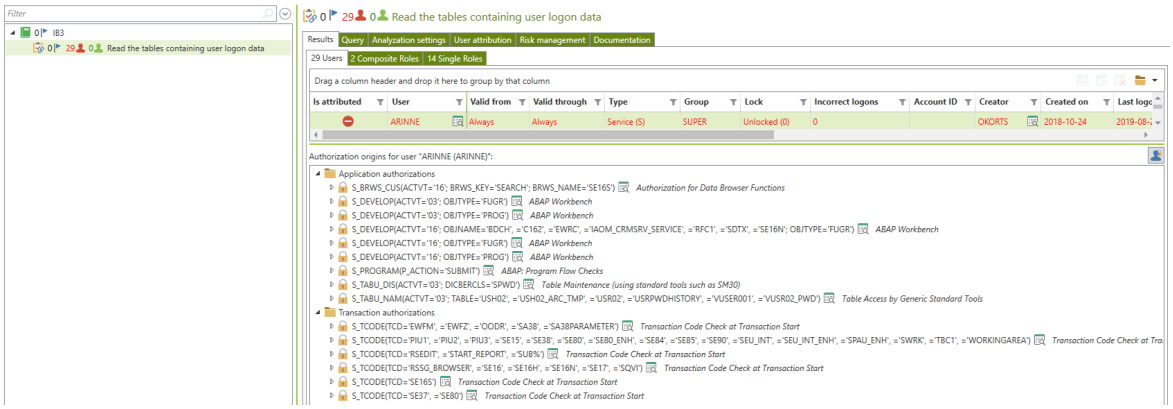


**Figure 66 - Result with non existing transaktions**

Another flag considers locked transactions. In every SAP system it is possible to create roles wich provide access to locked transactions. For security reasons SAP delivers this function and sometimes it is simply easier to lock a specific transaction instead of rebuilding the roles. To consider locked transactions in the authorization query evaluation, just activate the flag *locked transaction codes.*

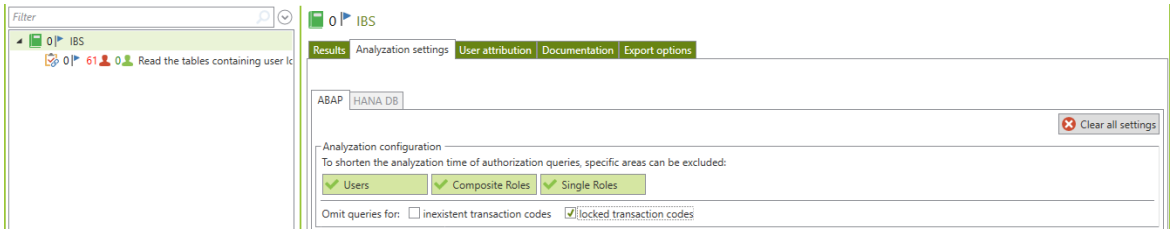


**Figure 67 - Auswahl Transaktion gesperrt**

In comparison to the evaluation results above, you can now see, that the transaction SE80 is missing in the authorization origin, because in this example SAP system, the SE80 transaction is locked.

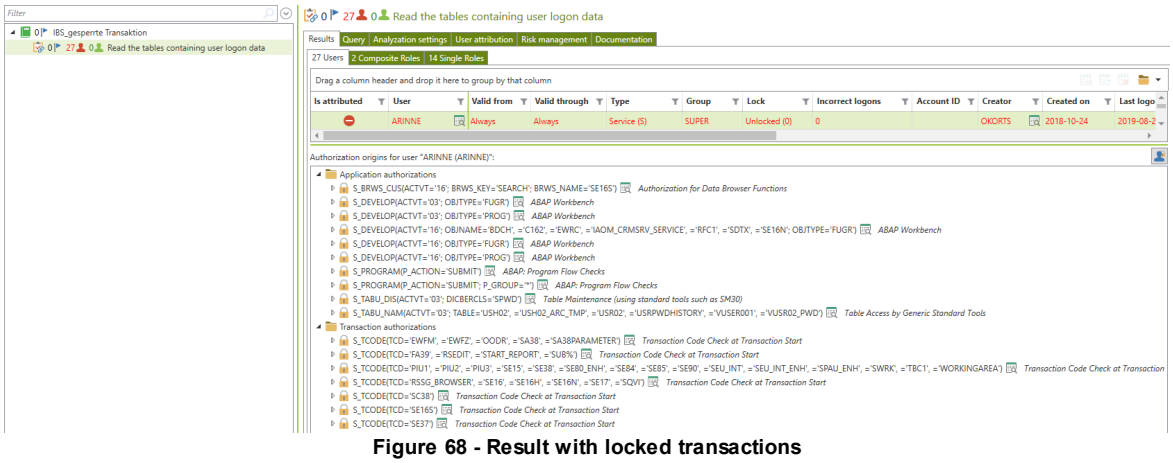


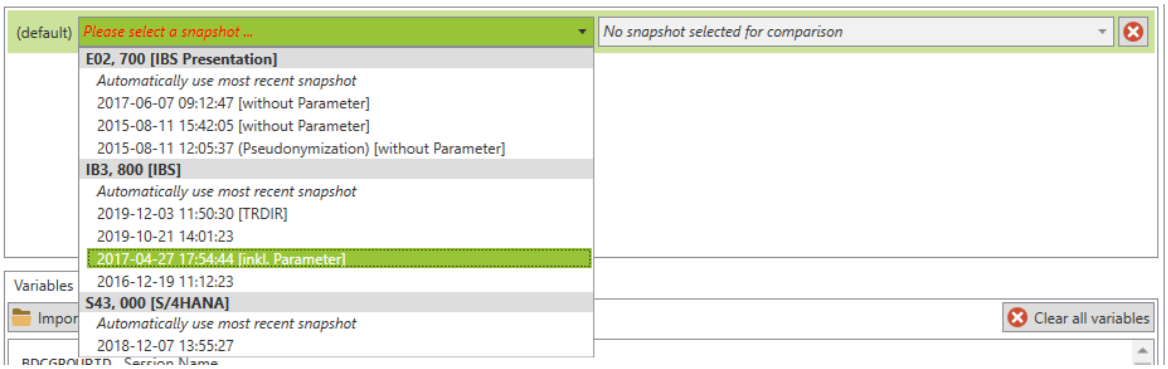
**Figure 68 - Result with locked transactions**

Both settings are useful in audits, when it's necessary to know, wich users are definitly able to execute critical processes in the SAP system. In this case users with acess to locked or non existing transactions will be filtered in the results.

In contrast, an analysis of the correct role settings, it is advisable to deactivate the flags considering non-existing or locked transactions to obtain an overall view of the correct role settings.

### III - 2.3.4 Snapshot / Snapshot comparison

To evaluate an analysis project, you must select the snapshot to be evaluated using the dropdown menu in the analysis settings:




**Fgure 69 - Selecting a snapshot**

You can select a specific snapshot directly by selecting the required date on which the snapshot was created or select a variable snapshot using the option Automatically use the most recent snapshot (Automatisch den jüngsten Snapshot verwenden). If there are multiple snapshots of the same system or client, this setting automatically selects the current version from the database. If this analysis setting is applied at the analysis project or folder level, then all subordinate elements inherit it as well.

You can also select an additional snapshot for comparison. The snapshot comparison helps you to perform follow-up checks (delta analyses of two snapshots of the same system). The results of this comparison relate only to the number of authorized users. This affords a simple overview of changes to user authorizations and facilitates user recertification.

To select the snapshot to be compared, the older snapshots of the system/client specified by the selected default snapshot are listed in the second dropdown menu.

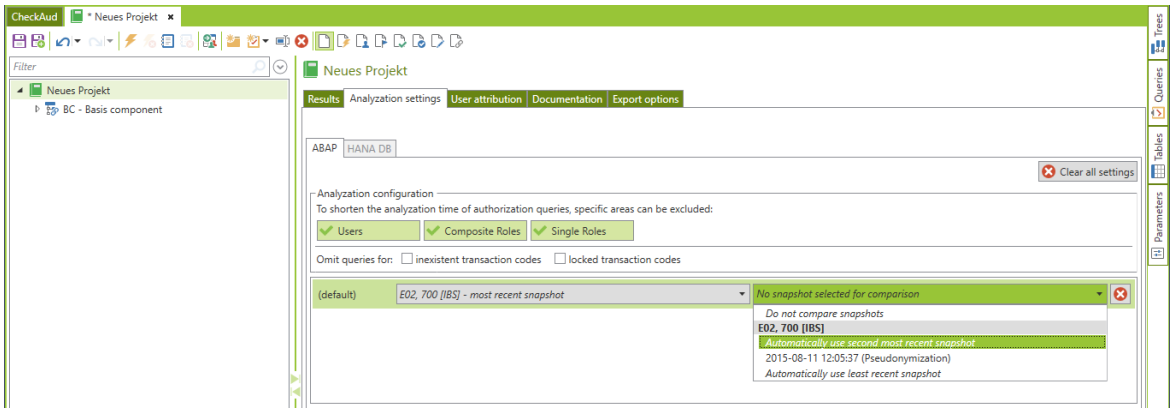



**Figure 70 - Selecting two snapshots for comparison**

If no other suitable snapshots are available in addition to the snapshot selected by default, then no selection for comparison is possible.

### III - 2.3.5 Variables - Variable check values in authorization queries

Authorization queries may contain variable check values. This feature is especially useful for queries at organizational level (for example, queries of who has an authorization in a specific company code). Variable check values are defined in the analysis settings. In the authorization queries, these values are highlighted by the word *variable* (graphical view) and the character $ (technical view) in the field value definitions of an authorization object.

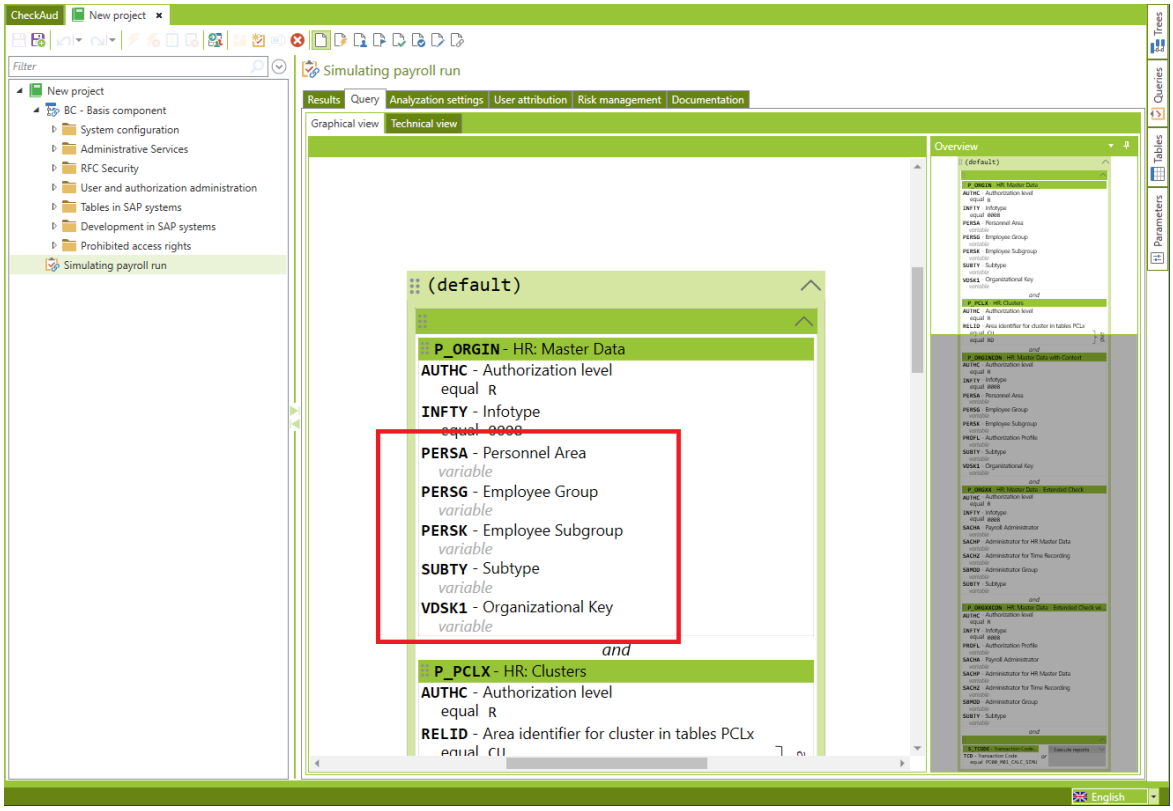



**Figure 71 - Variable field values in the graphical view**

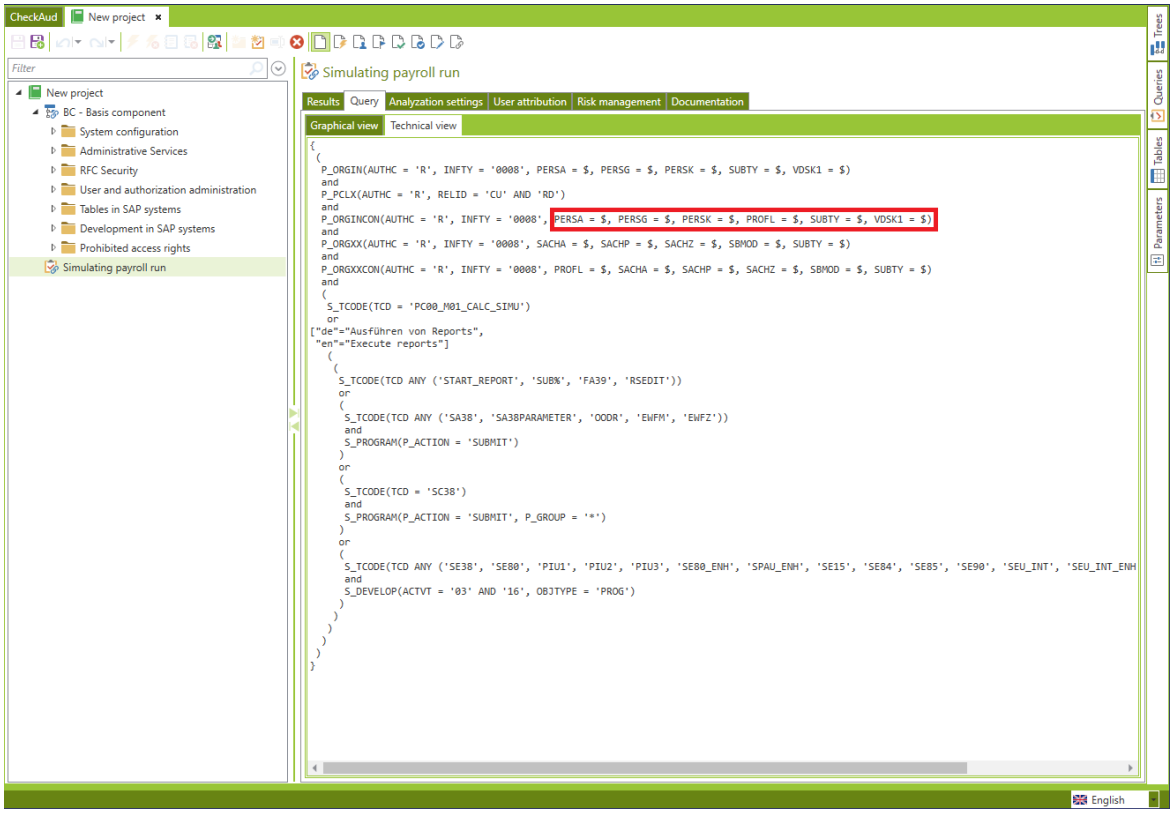



**Figure 72 - Variable field values in the technical view**

If you select a snapshot in the *Analysis settings* and the authorization queries of the analysis project or selected folder contain variable check values, these check values are listed on the *Variables* tab:

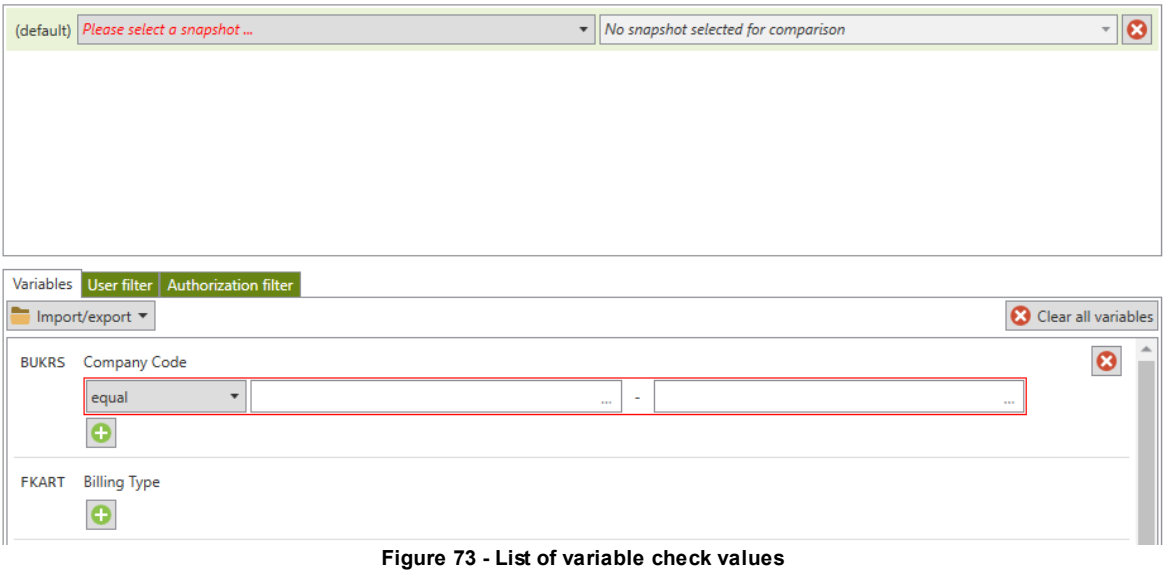



**Figure 73 - List of variable check values**

You can define variable check values using the  button. When doing so, you must also define the logical relational operator in addition to the field value:

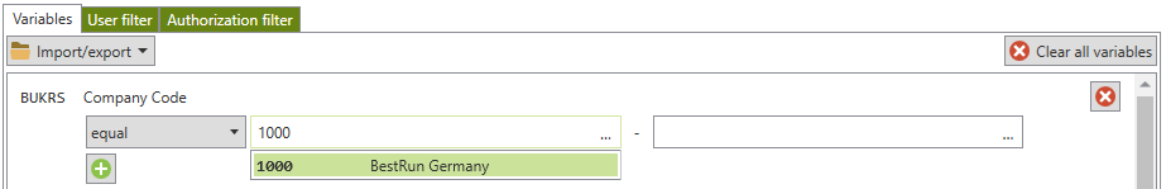



**Figure 74 - "equal" relational operator for field values**

This operator is used to query whether an authorisation contains any value within the specified interval. The specified values are always inclusive. The following query displays all authorizations in which the Transaction Code (S_TCODE) field contains a value between RZ and RZ99.

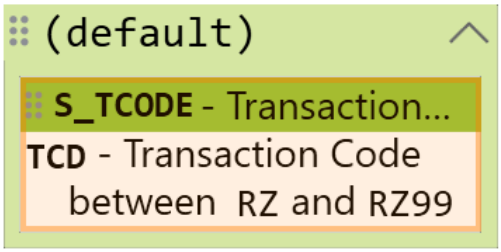



**Figure 75 - "betweenI" relational operator for field values**

```
{
 S_TCODE(TCD BETWEEN 'RZ' AND 'RZ99')
}
```

**Figure 76 - "betweenI" relational operator for field values**


**Figure 77 - "like" relational operator for field values**


**Figure 78 - "all" relational operator for field values**


**Figure 79 - "any" relational operator for field values**

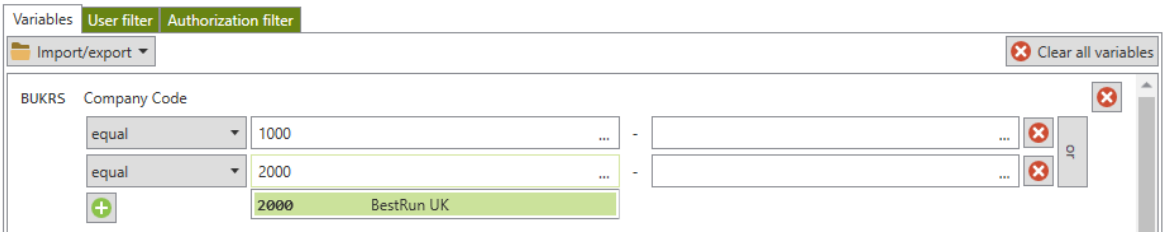



**Figure 80 - "equal" relational operator for two field values**

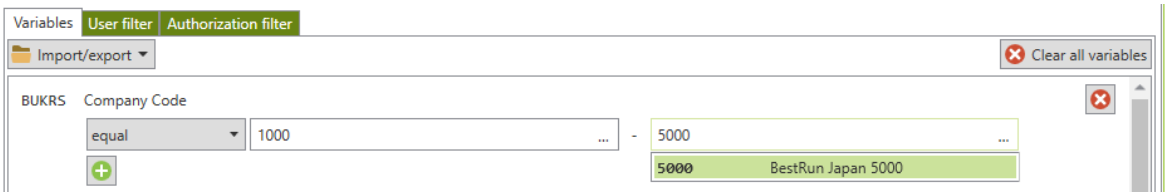
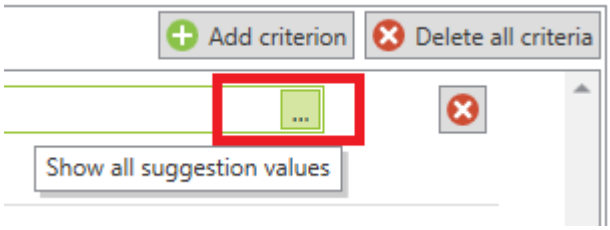



**Figure 81 - "equal" relational operator for field values from/to**

**Note:** The input fields for the comparison criteria have a search and auto-complete feature. Suitable suggestions for the field are provided for selection.




When you click the ... button, an additional dropdown menu with a list of the available field values opens. This function is available only if the option *Read out default values for org levels* for creating the snapshot is enabled in the scan module.

You can find a detailed description of the available relational operators in the chapter Relational Operators for Field Values.

You can use the Import/export button to load or save variable sets. If this analysis setting is applied at the analysis project or folder level, then all subordinate elements inherit it as well.

After the predefined filter settings are exported, they are available for quick access using the Import/export button. Select a file to load the filter settings to CheckAud..

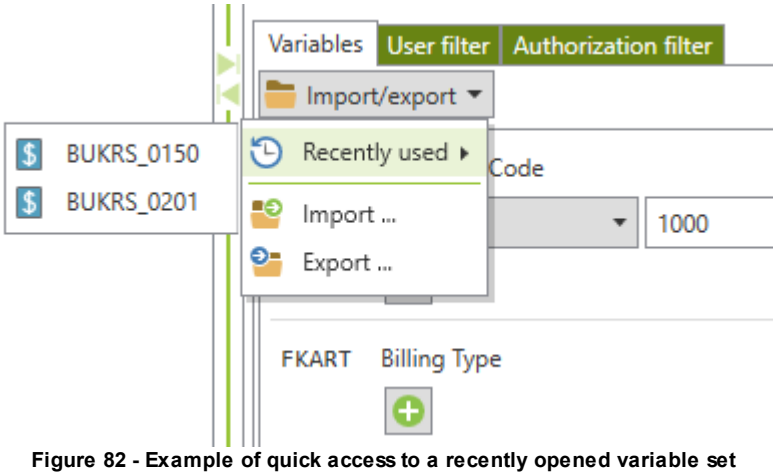



**Figure 82 - Example of quick access to a recently opened variable set**

**Note:** The filter settings last used remain in the list even after you close the project or the software.

**Note:** CheckAud interprets special definitions of variable field values as follows, for example:

*Authorization object F_LFA1_BUK, field BUKRS = $*
The field BUKRS is not defined, which means that it is not included in the authorization check.

*Authorization object F_LFA1_BUK, field BUKRS = "*"*
The field BUKRS is defined with "*", which means that the system searches only for users that have received the authorization object F_LFA1_BUK with the field BUKRS defined as "*".

*Authorization object F_LFA1_BUK, field BUKRS like "*"*
The field BUKRS is defined with "like *", which means that the system searches only for users who have received the authorization object F_LFA1_BUK with BUKRS defined as any field value. As a result, all the assigned field values for this user are listed here.

**Note:** the Tab Variables is only shown when ABAP systems are selected

### III - 2.3.6 User filters

You can use user filters to include or exclude specific users in the analysis. You can configure the analysis settings on the User filters tab. To use this feature, you must first select a snapshot for the analysis project/the element in the analysis project, because this setting is dependent on the characteristics in the SAP system snapshot:

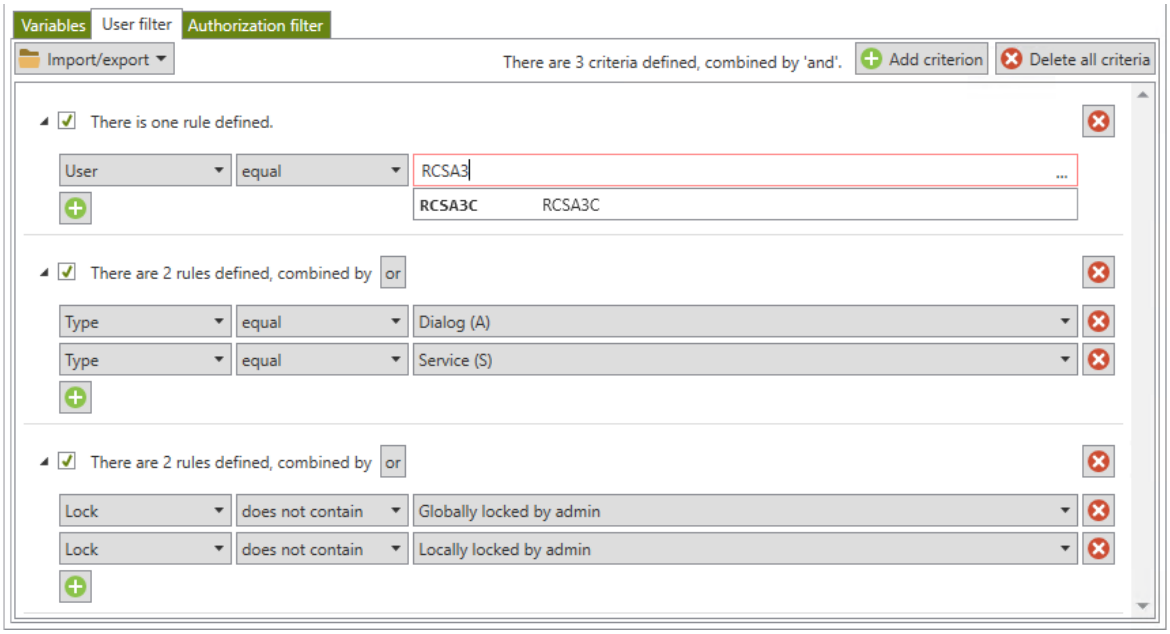



**Figure 83 - User filter for the analysis**

You can define inclusion and exclusion criteria for defining the user filter.

The following attributes for ABAP systems are available as criteria:
- User
- Type
- Lock
- Valid from
- Valid to
- Group
- Department
- Function

The following attributes for HANA DB systems are available as criteria:
- User
- Valid from
- Valid to
- Restricted
- Deactivated
- User group

The following relational operators are available for the filter criteria (depending on the attribute):
- Equal
- Not equal to
- Between
- Not between
- Like
- Unlike
- Includes
- Does not include
- Less than

- Greater than
- Less than or equal to
- Greater than or equal to

If this analysis setting is applied at the analysis project or folder level, then all subordinate elements inherit it as well.

If no filter criteria have been defined yet, standard filters are provided for selection. You can activate them using the Click here to select a standard filter button.

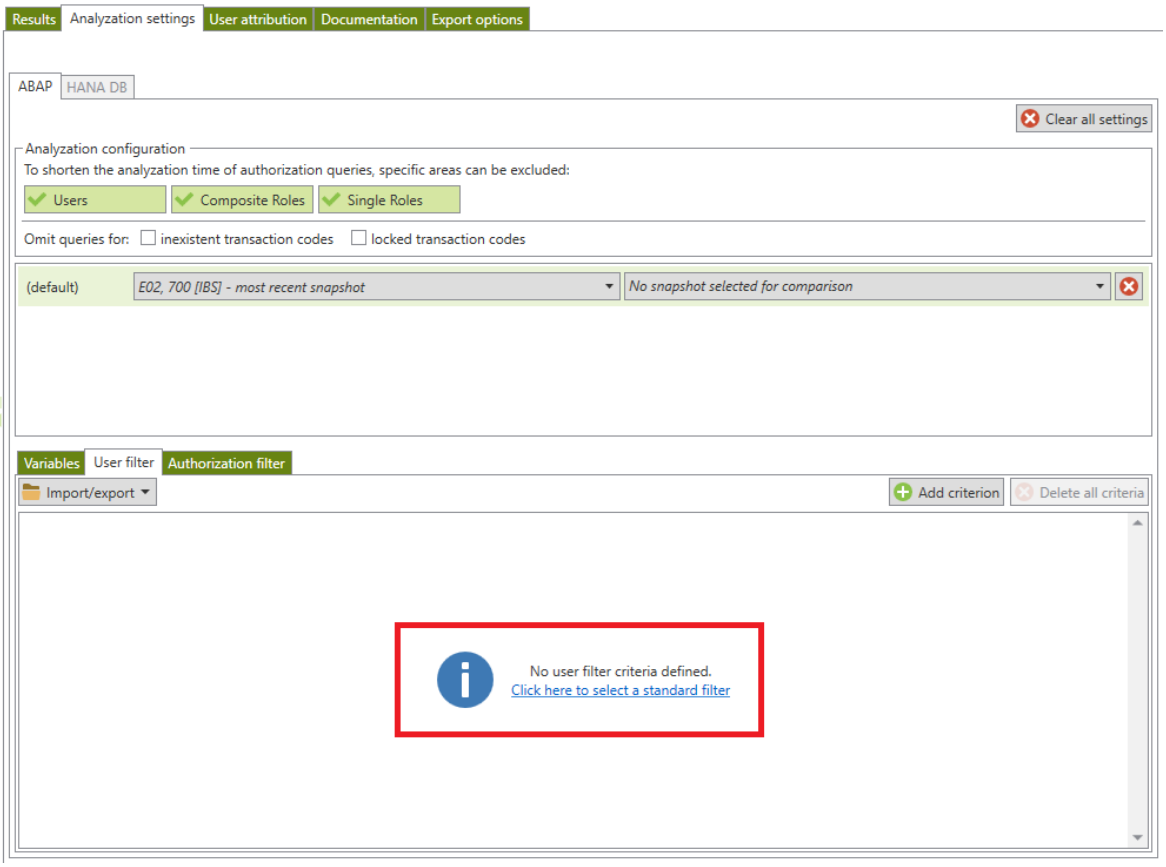
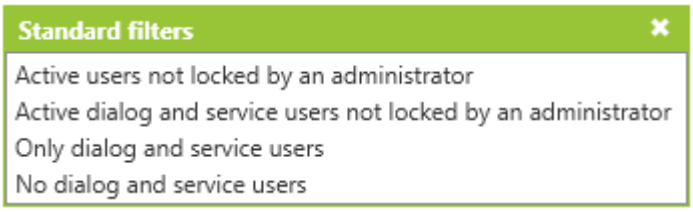



**Figure 84 - Predefined user filters**

The following standard filters for ABAP systems are available for selection:



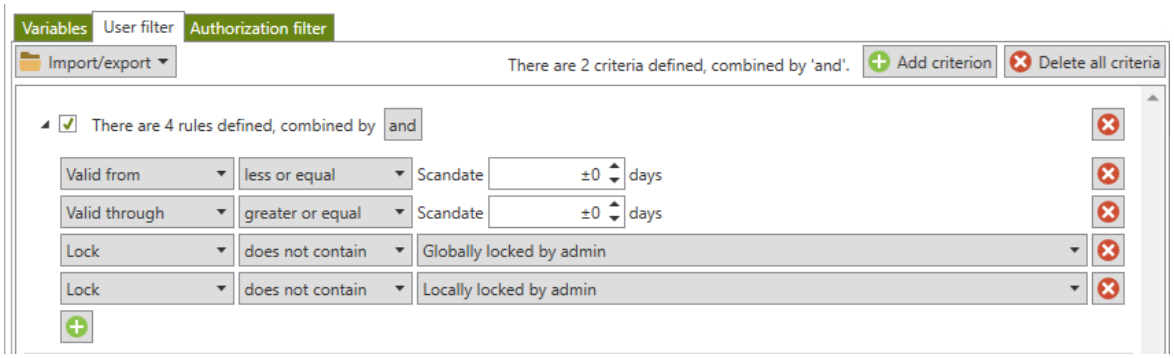



**Figure 85 - Active users (not locked by admin)**

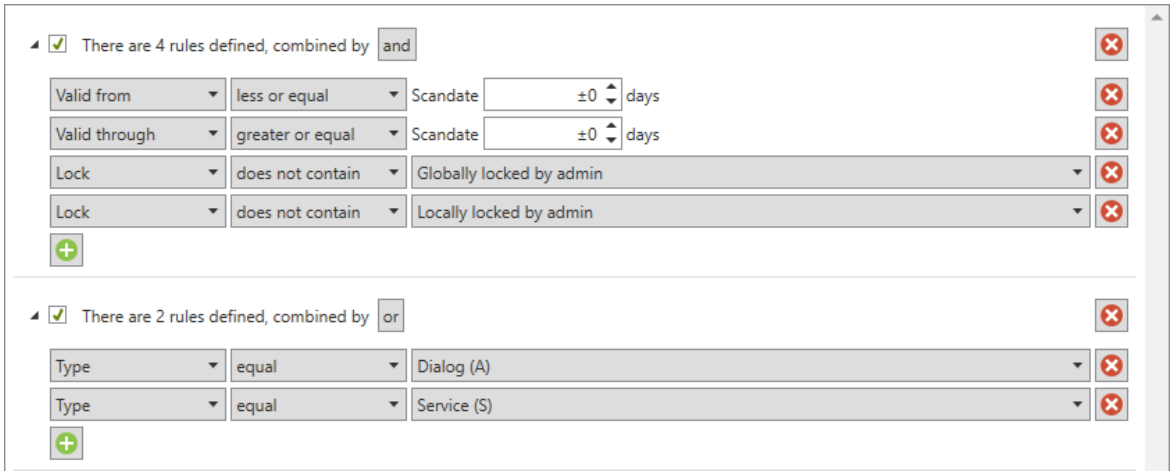



**Figure 86 - Active dialog and service users (not locked by admin)**

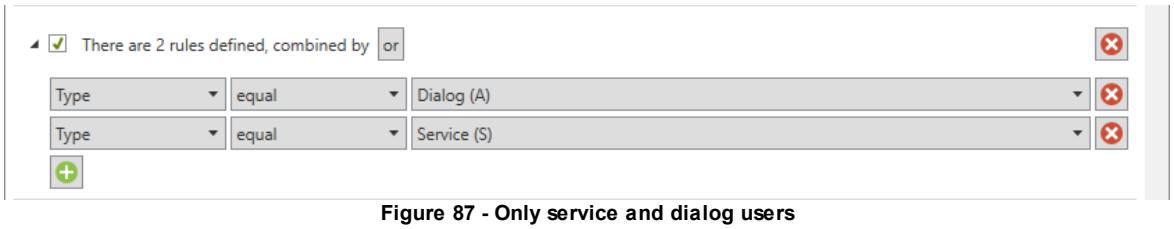



**Figure 87 - Only service and dialog users**

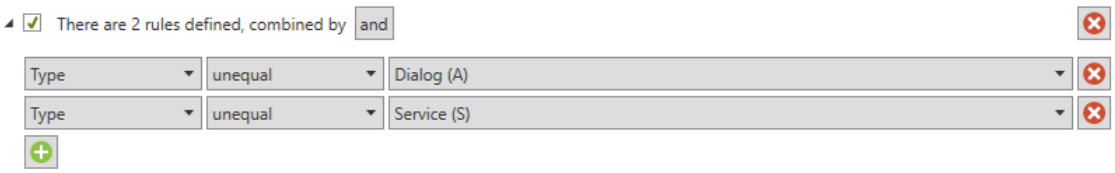



**Figure 88 - No service or dialog users**

You can use the 

button to load or save filters. An import of filter criteria from a TXT file is also available for selection. You can use this feature to import multiple filter settings (for example, for user IDs) quickly. The TXT file may contain only one user ID per line:

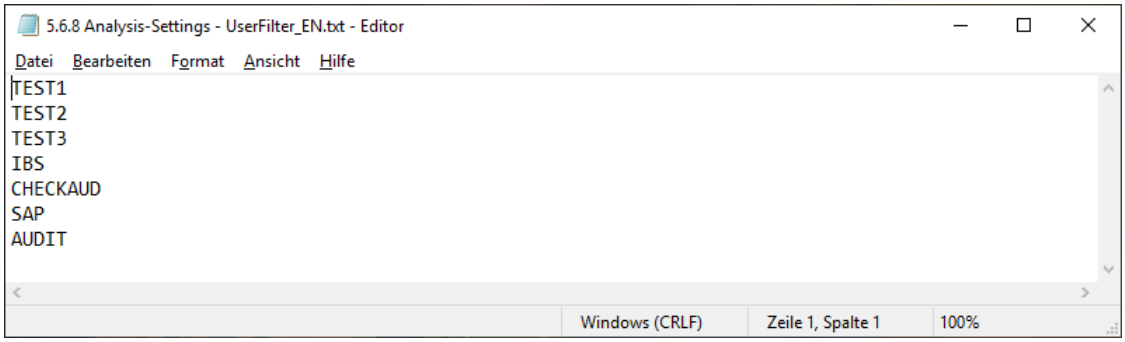



**Figure 89 - TXT file with the user IDs for SAP**

Choose the 

button to open a dialog window for selecting saved user filters. Here, the file format must be changed from **.causerfilter to* *.txt:

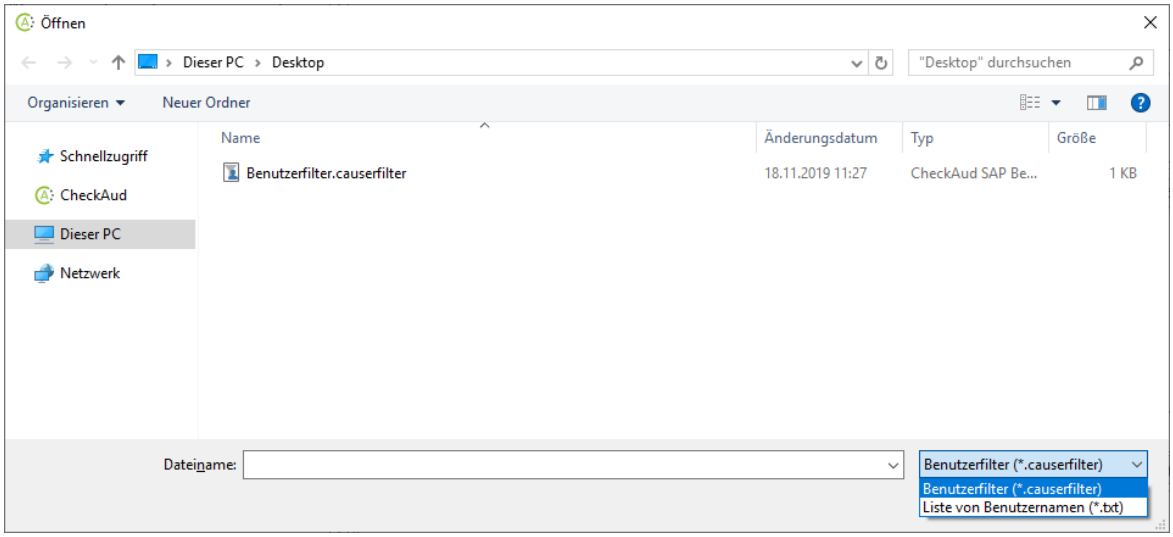



**Figure 90 - Changing the file type**

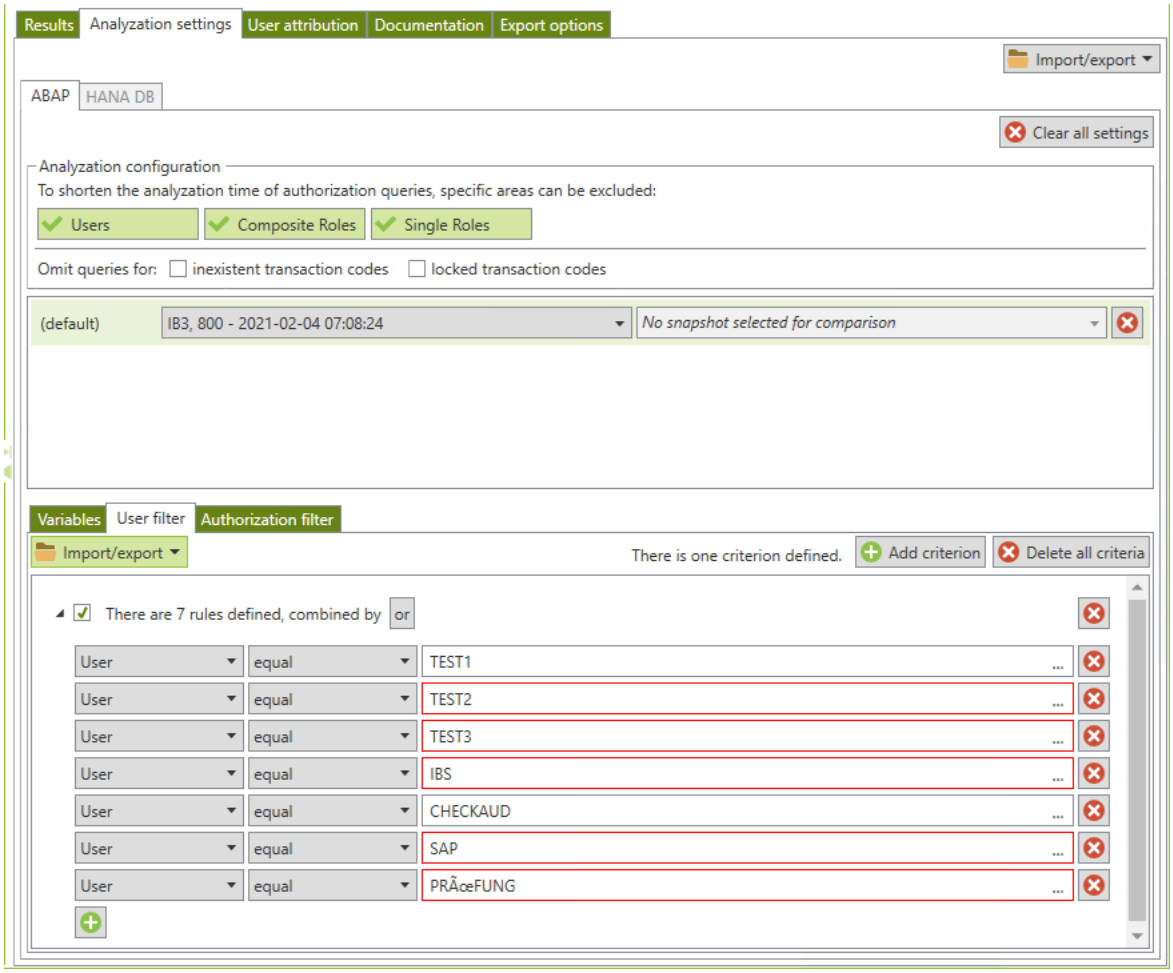
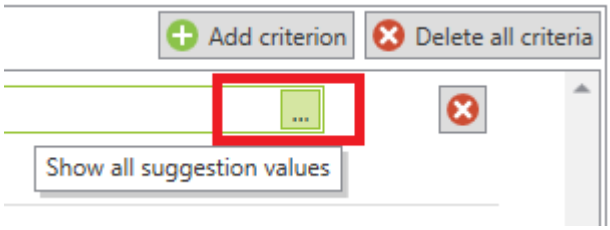



**Figure 91 - Using an imported TXT file as a filter definition**

**Note:** The input fields for the comparison criteria have a search and auto-complete feature. Suitable suggestions for the field are provided for selection.




When you click the ... button, an additional dropdown menu with a list of the available field values opens.

When using the two filter criteria "like" or "not like", the configuration of the filtering can be specified with the special characters "*", "?", "+" as well as "\". The special character "*" means that any number of additional characters are subsequently searched for and taken into account in the evaluation.

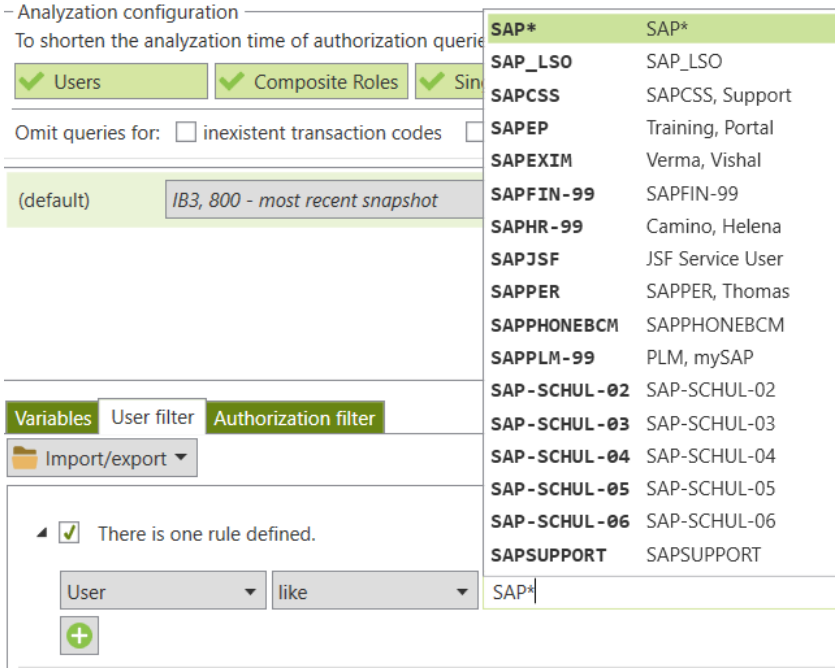



**Figure 92 - Query with special character "*"**

The special character "?" means that exactly 1 additional character is subsequently searched for and taken into account in the evaluation.

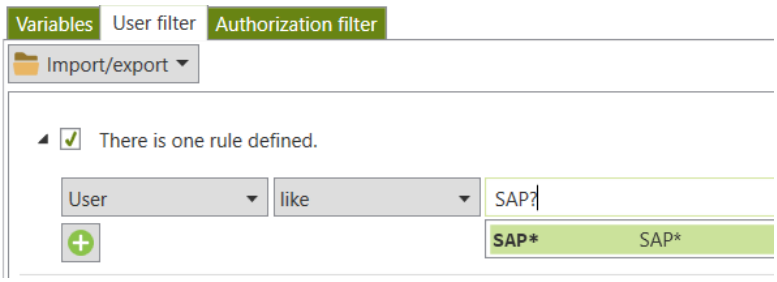



**Figure 93 - Query with special character "?"**

The special character "+" means that at least 1 additional character is searched for subsequently and taken into account in the evaluation.

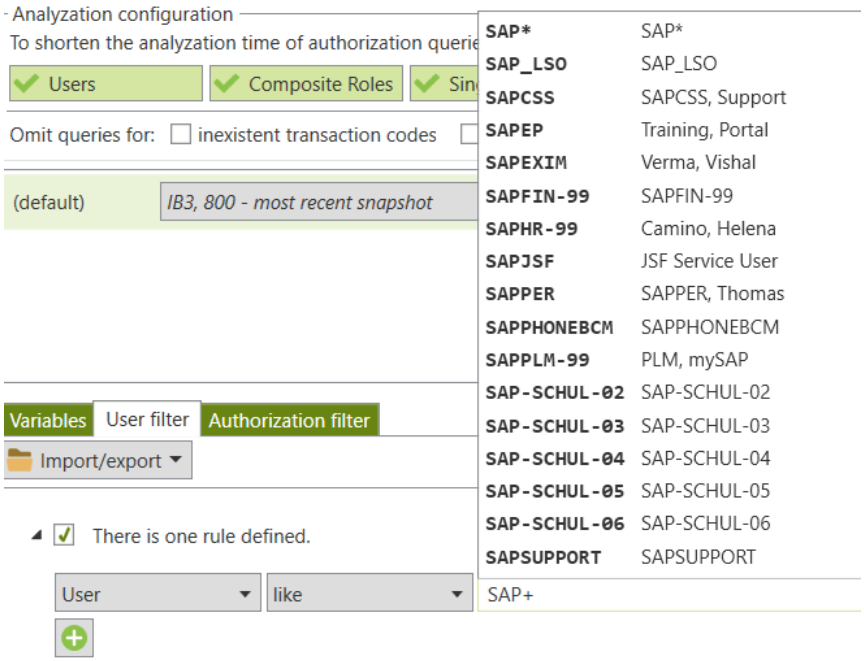



**Figure 94 - Query with special character "+"**

The use of the special character "\" is required if a special character, such as "*", "?" or "+" occurs in the name and the use cases described above are to be switched off, so to speak.

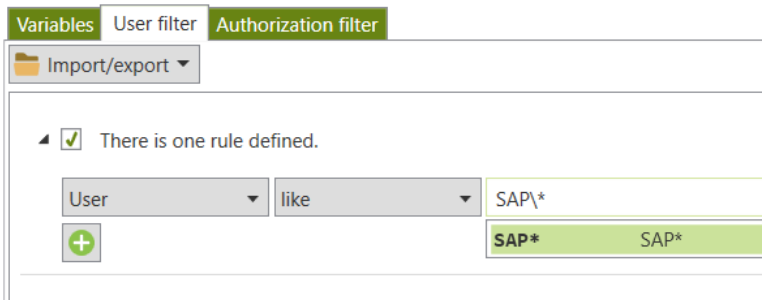



**Figure 95 - Query with special character "\"**

### III - 2.3.7 Authorization filter

You can use the authorization filter to assess or hide specific roles or profiles for the evaluation of authorization origins. For instance, the composite profile *SAP_ALL* can be hidden in the evaluation of authorization origins. As a result, only users who have received the authorization under inspection from somewhere other than the composite profile *SAP_ALL* are displayed.

You can define inclusion and exclusion criteria for defining the authorization filter. For the authorization filter, the following authorization origin criteria are available:

- Single profile
- Group profile
- Individual role
- Group role

- Reference

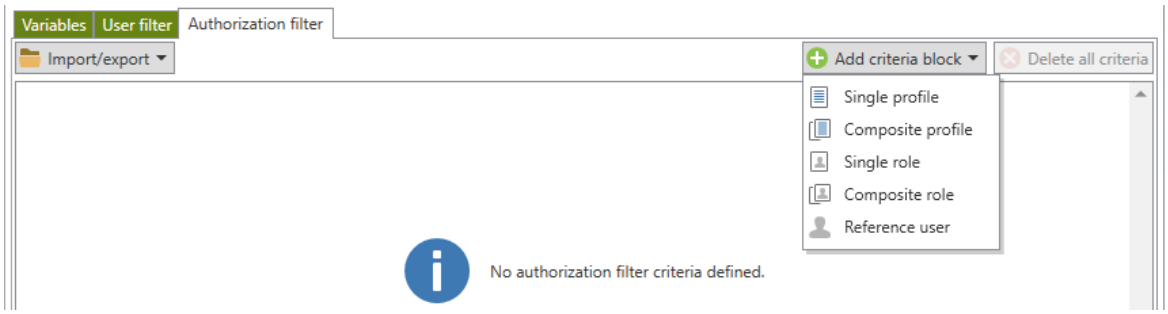



**Figure 96 - Criteria block for authorization filter**

The following relational operators are available for the filter criteria:

- Equal
- Not equal to
- Between
- Not between
- Like
- Unlike


**Figure 97 - Relational operators for filter criteria**

For the filter criteria, there is also a differentiation between inclusion and exclusion criteria:

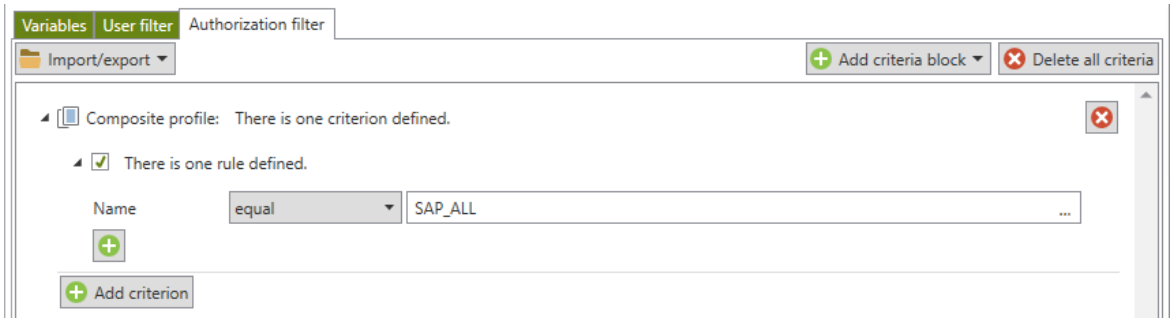



**Figure 98 - Inclusion criteria**

Users with the profile *SAP_ALL* and users with one or more authorized roles/one or more authorized reference users are displayed. Users that are only authorized through their profile assignments and do not have *SAP_ALL* are not displayed.


**Figure 99 - Inclusion criteria**

Here, the users who have received the analyzed authorization via group profiles that partially or completely match the profile designation entered are displayed. The relational operator can be used with the wildcard * at the end of the string.

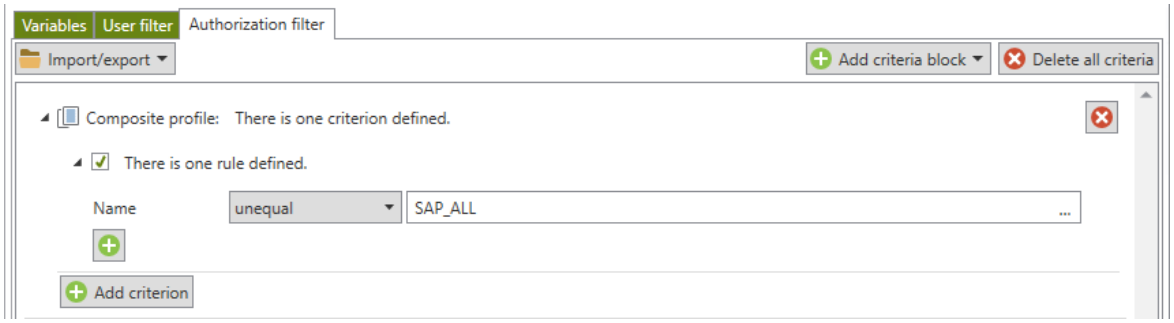


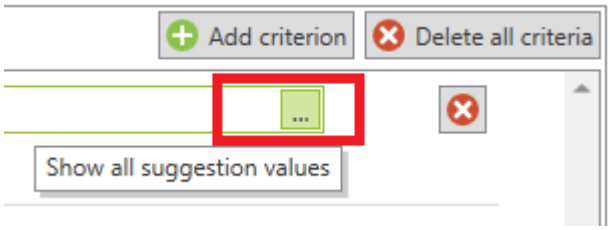

**Figure 100 - Exclusion criteria**

The results will only show users who have not received the analyzed authorization exclusively via the SAP_ALL group profile.


**Figure 101 - Exclusion criteria**

The results will only show users who have not received the analyzed authorization exclusively via group profiles with the string SAP.

**Note:** The input fields for the comparison criteria have a search and auto-complete feature. Suitable suggestions for the field are provided for selection.




When you click the ... button, an additional dropdown menu with a list of the available field values opens.

**Note:** authorization filters are yet only available for ABAP systems

## III - 2.4 Inheriting analysis settings

An analysis project can be set up quickly and efficiently by inheriting analysis settings. Analysis settings can be configured at project, folder or query level:

Project level: Settings are inherited to all subelements.

Folder level: Settings are adopted from the inheritance; alternatively, the inheritance can be interrupted at folder level. In such a case, the new settings are inherited to all lower-level elements starting from this level.

Query level: Settings are adopted from the inheritance; alternatively, the inheritance can be interrupted at query level. In such a case, separate settings then apply for these queries.

The inheritance is used to pass on analysis settings (the selection of the snapshot, variable specifications and filter settings). You can interrupt the inheritance to the individual subelements in general by removing the flag *Inherit system assignment, variables and filters*.

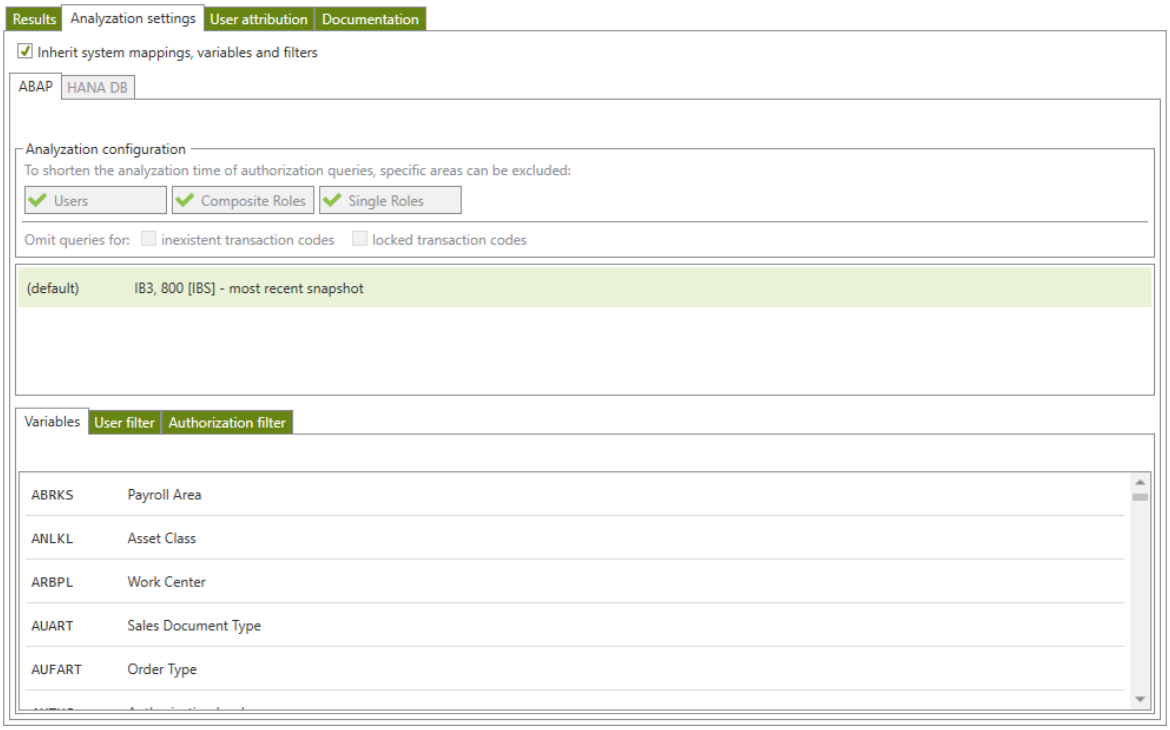



**Figure 102 - Inheritance activated, settings are transferred**

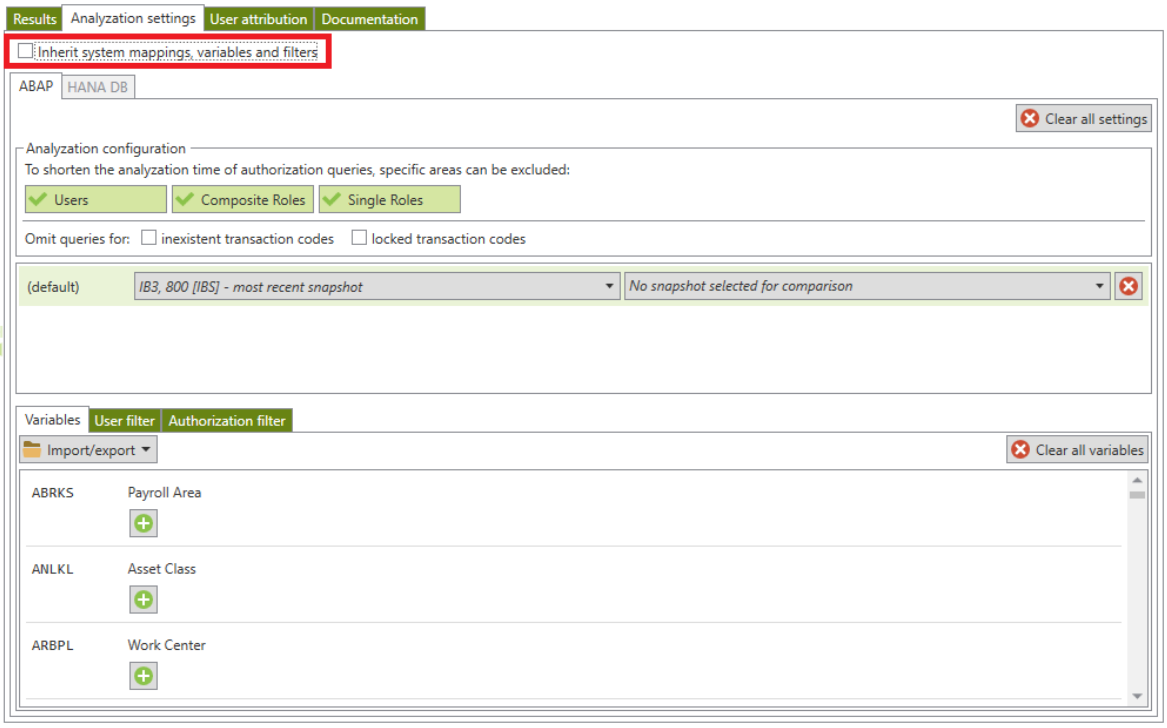



**Figure 103 - Inheritance interrupted, settings are individual starting from this level**

You can then set new snapshot settings, variables and filters for this level.

To make it easy to identify inheritance interruptions in the analysis project, you can change the view in the analysis project.

Default analysis project view

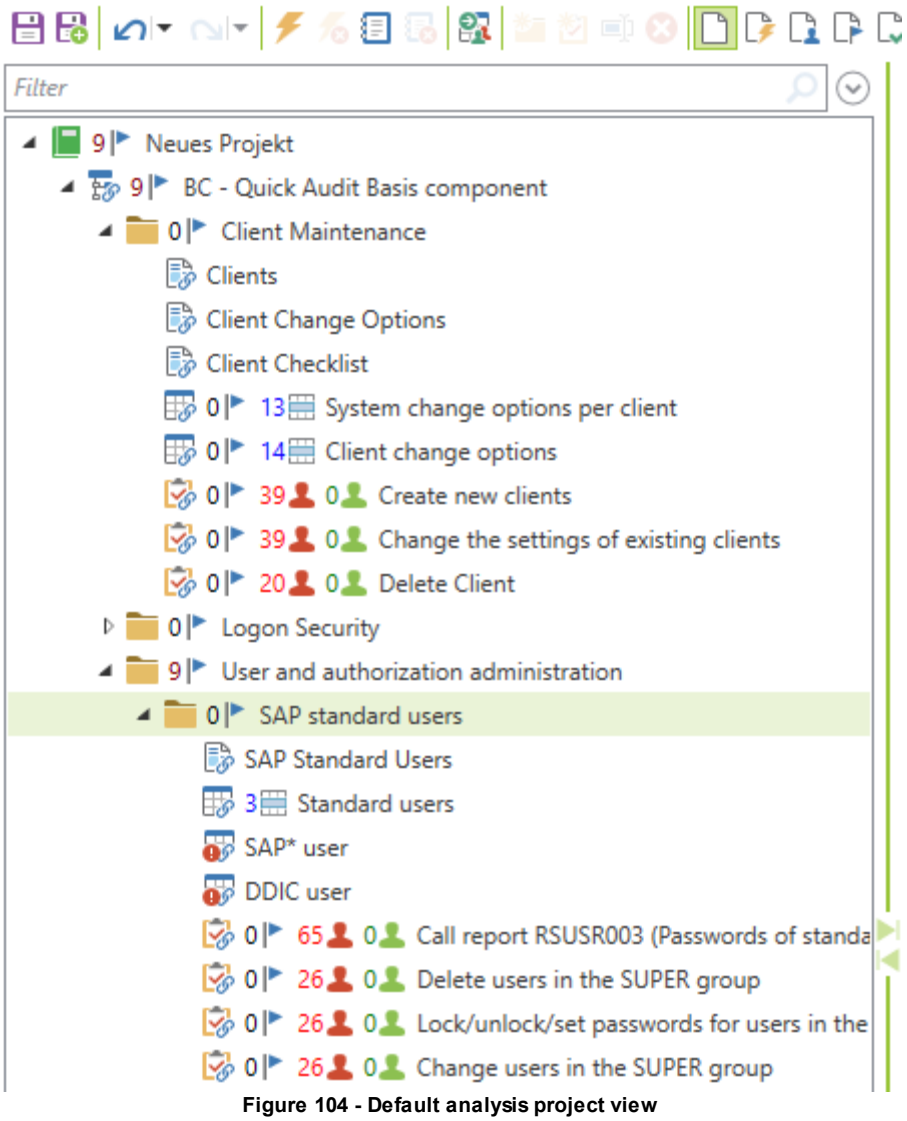



**Figure 104 - Default analysis project view**

Making interruptions of inheritance in the analysis settings known in the analysis project view

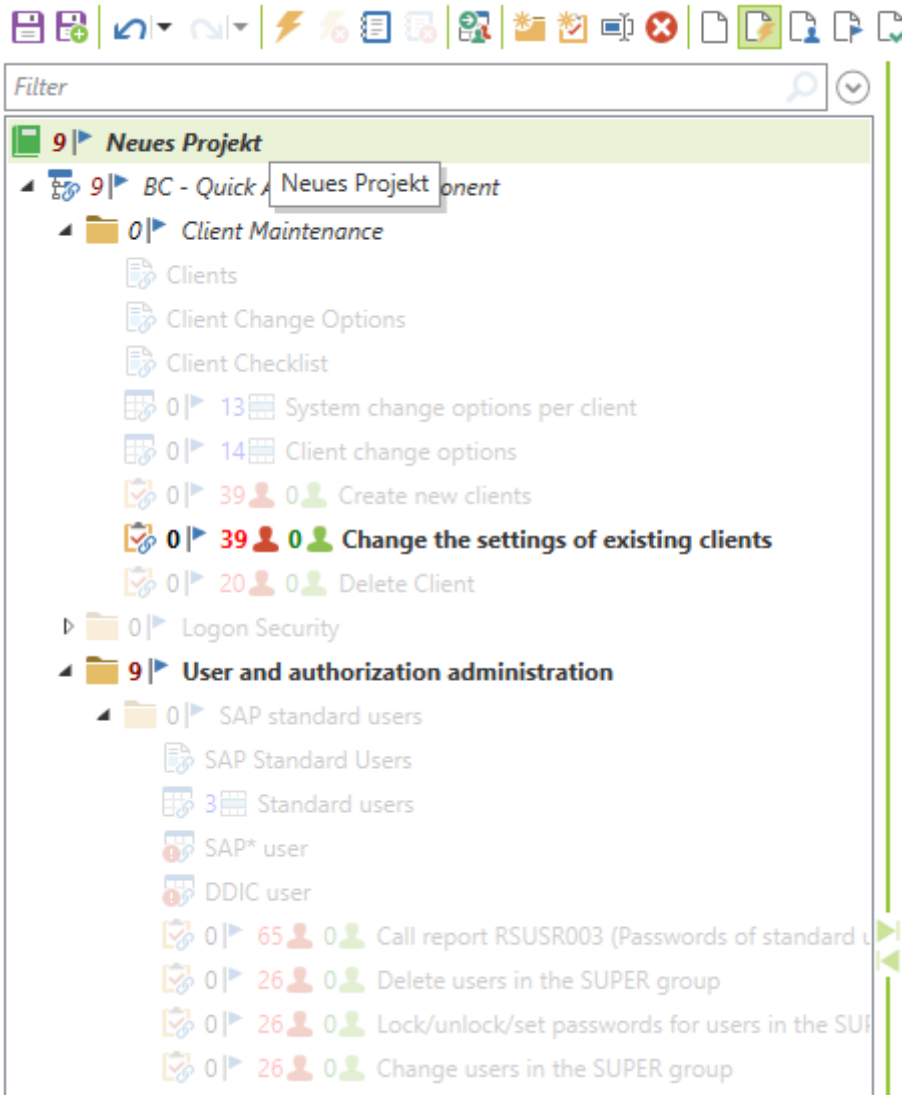



**Figure 105 - Displaying an inheritance interruption in the analysis settings of the analysis project**

If the inheritance of the analysis settings is interrupted in individual queries or folders, the interruption can be viewed using this feature.

## III - 2.5 Filtering in the analysis project view

In complex analysis projects, it is helpful to use the search function to display elements that you are looking for. For instance, you can display elements filtered by name, keyword, included authorization objects, transactions, tables and parameters in the analysis project view. This function is located in the input field above the analysis project.

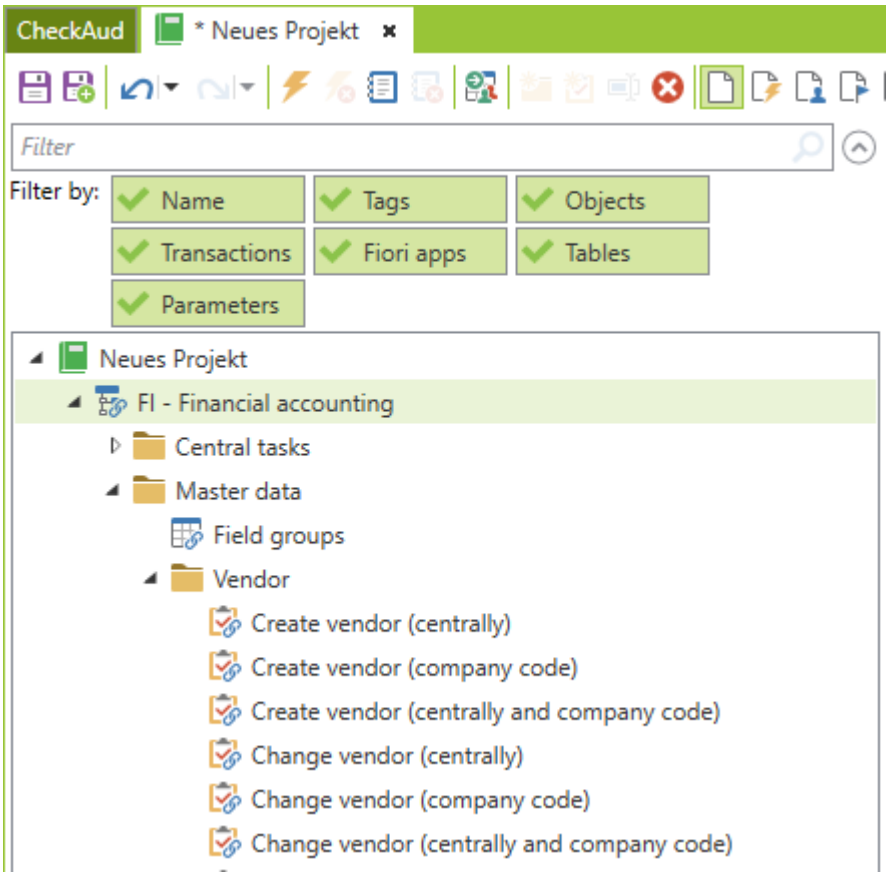



**Figure 106 - Filtering in the Analysis Project**

## III - 2.6 Multilingual analysis projects

The analysis projects are also maintained in several languages. The standard systems supplied by IBS are available in German and English. You have to maintain your own analysis projects and the contents that you create in other languages. The contents (query names, risk descriptions, messages, etc.) can be edited intuitively in German and English.

Some of the elements in the analysis project (folders or queries) can be renamed using the button. When you use this feature, you can make your entry in both German and English:

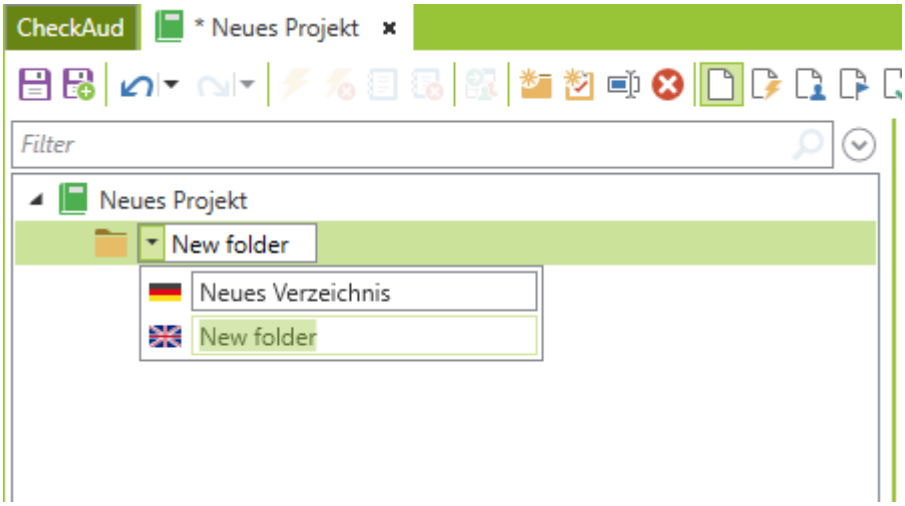



**Figure 107 - Analysis projects with multiple languages**

More detailed information about queries, such as risk descriptions, documentation, and so on, can be maintained in the respective languages using the Deutsch or English buttons.

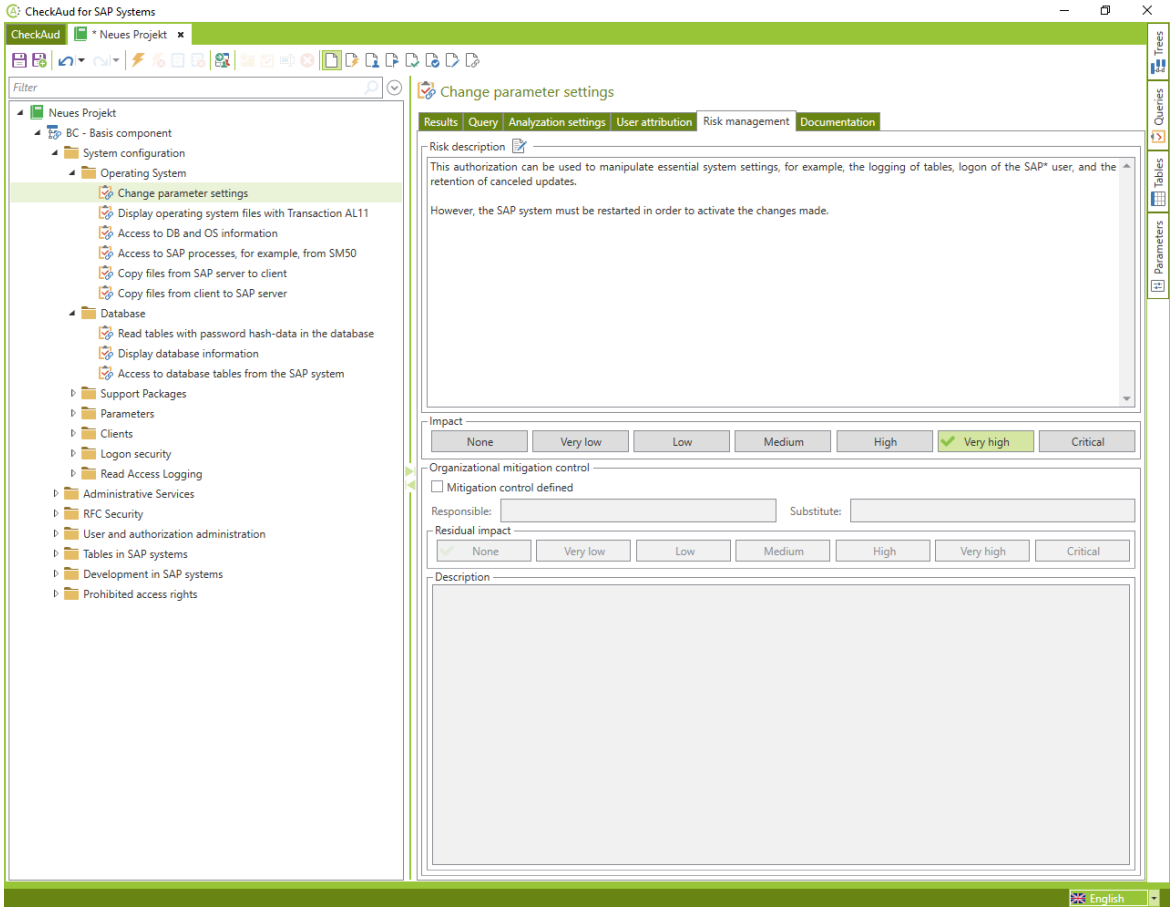



**Figure 108 - Maintaining documentation in Englisch**

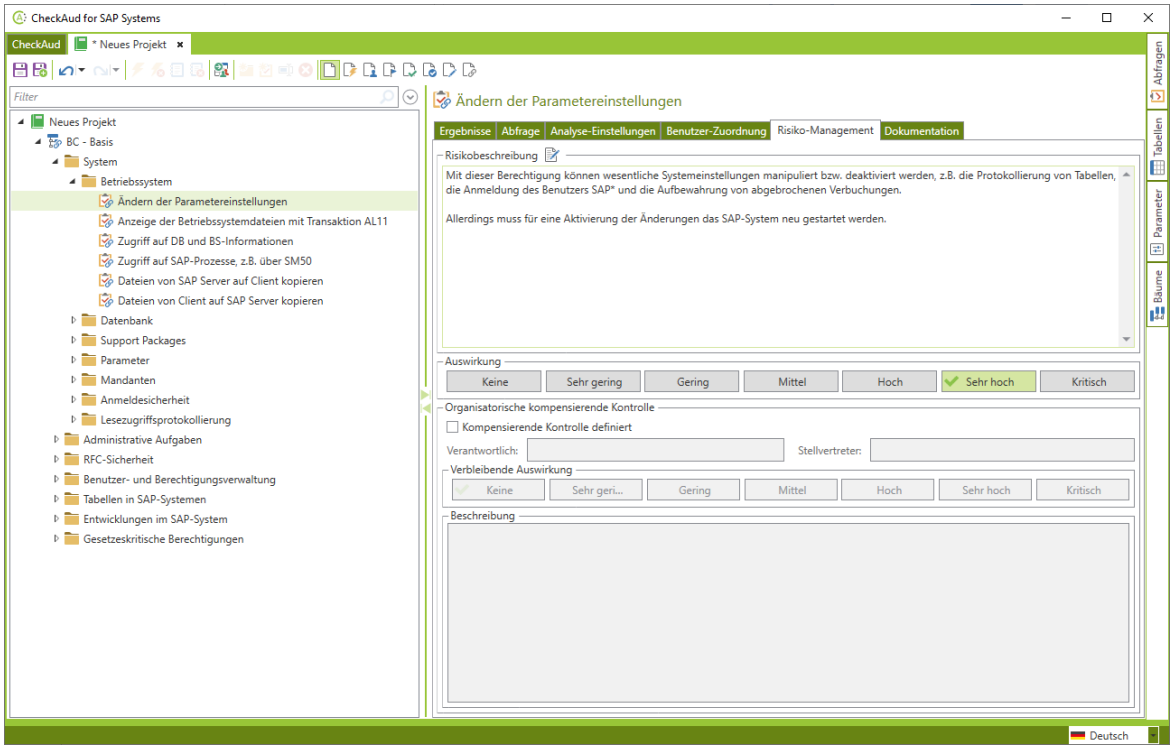



**Figure 109 - Maintaining documentation in German**

## III - 3 Performing an analysis

You can perform an analysis for an individual query (authorization query, table query, parameter query) or for multiple queries as part of a subproject or the overall analysis project. The evaluation can be performed only if a snapshot has been assigned for at least one query in the analysis project.

## III - 3.1 Evaluating an authorization query (ABAP)

To evaluate an individual authorization query, you must select it in the project. You can then start the evaluation for this authorization query using the *Analyze now* button on the *Results* tab.

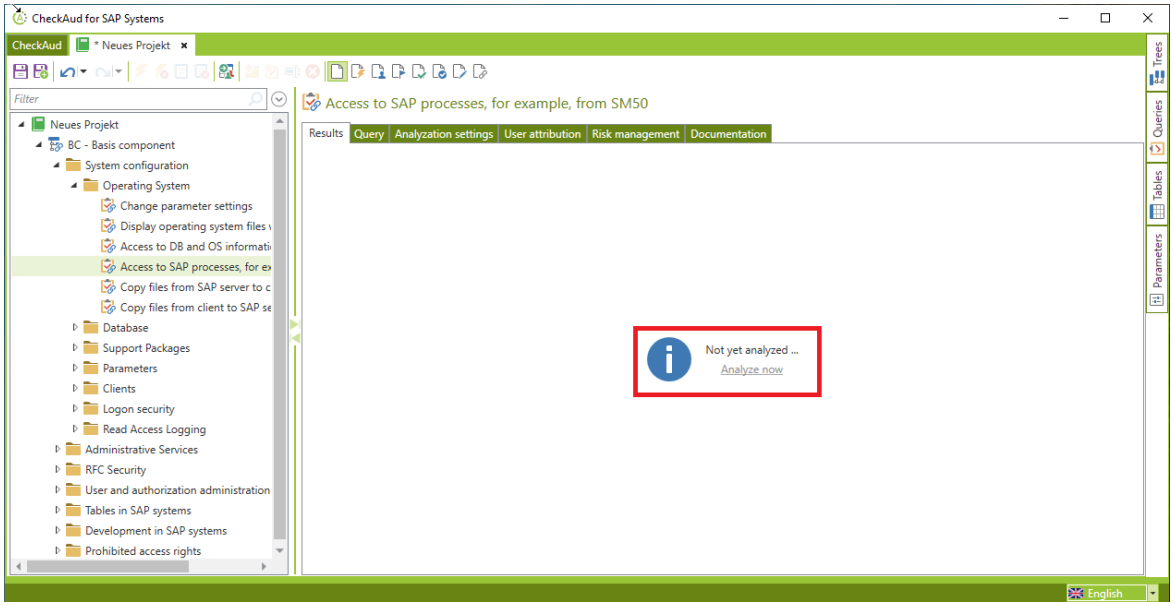



**Figure 110 - Evaluating an authorization query**

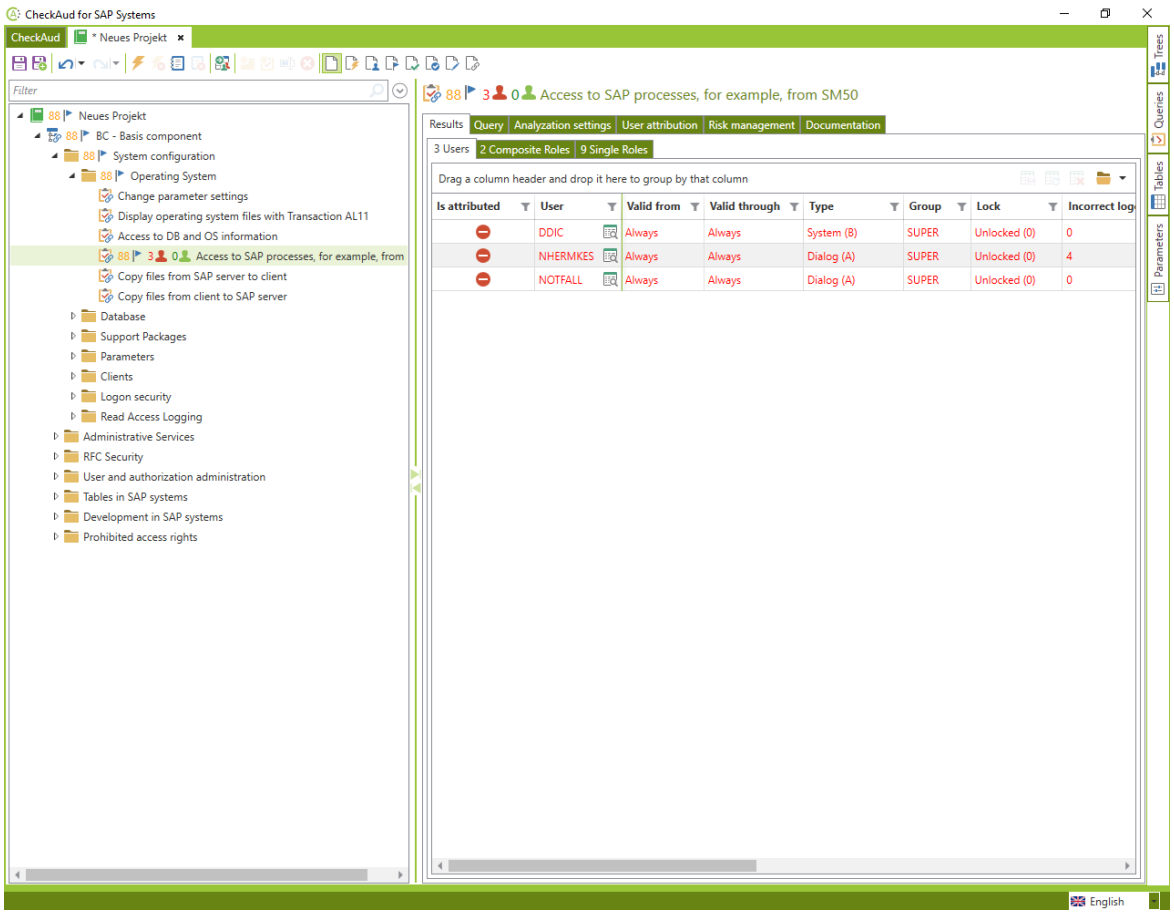



**Figure 111 - An evaluated authorization query**

Alternatively, the selected authorization query can be evaluated by choosing the button and the evaluation can be stopped by choosing the button.

Evaluated authorization queries are shown through the key figures in the results:

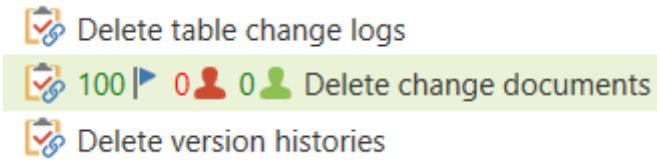
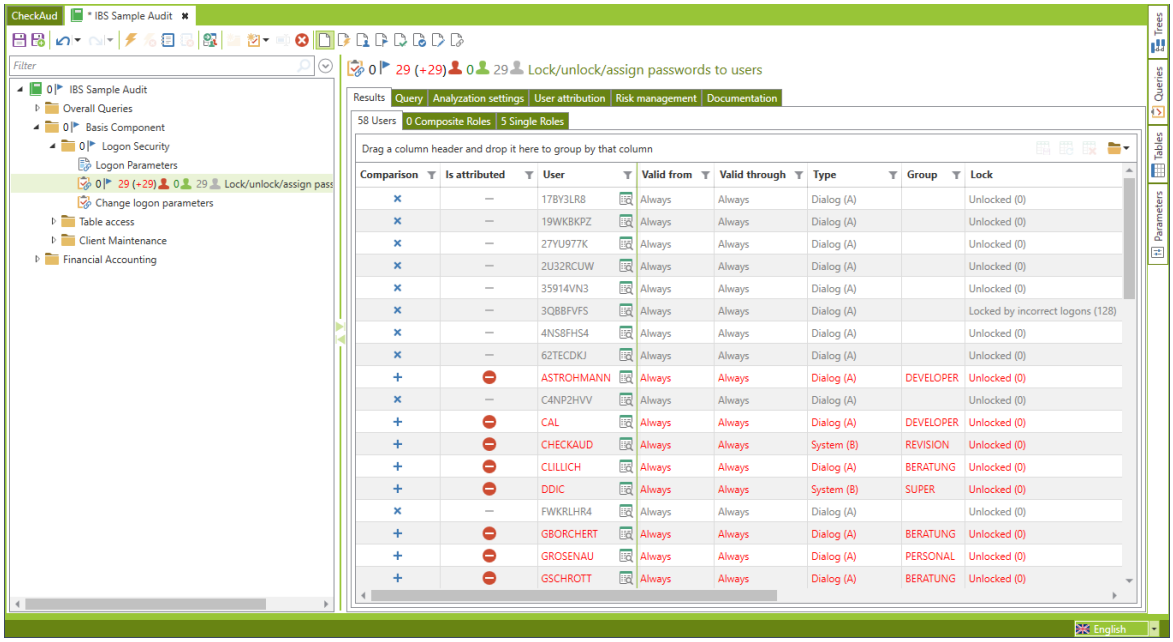



**Figure 112 - An evaluated authorization query**

If an additional snapshot was selected for comparison for the evaluation, the results of the comparison are displayed as follows:



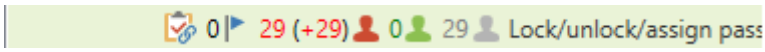




**Figure 113 - Evaluated authorization query, comparison of two snapshots**

Detailed information about the displayed results can be found in the chapter *Results Displayed in the Analysis Project*.

## III - 3.2 Evaluating an authorization query (HANA DB)

To evaluate an individual authorization query, you must select it in the project. You can then start the evaluation for this authorization query using the *Analyze now* button on the *Results* tab.

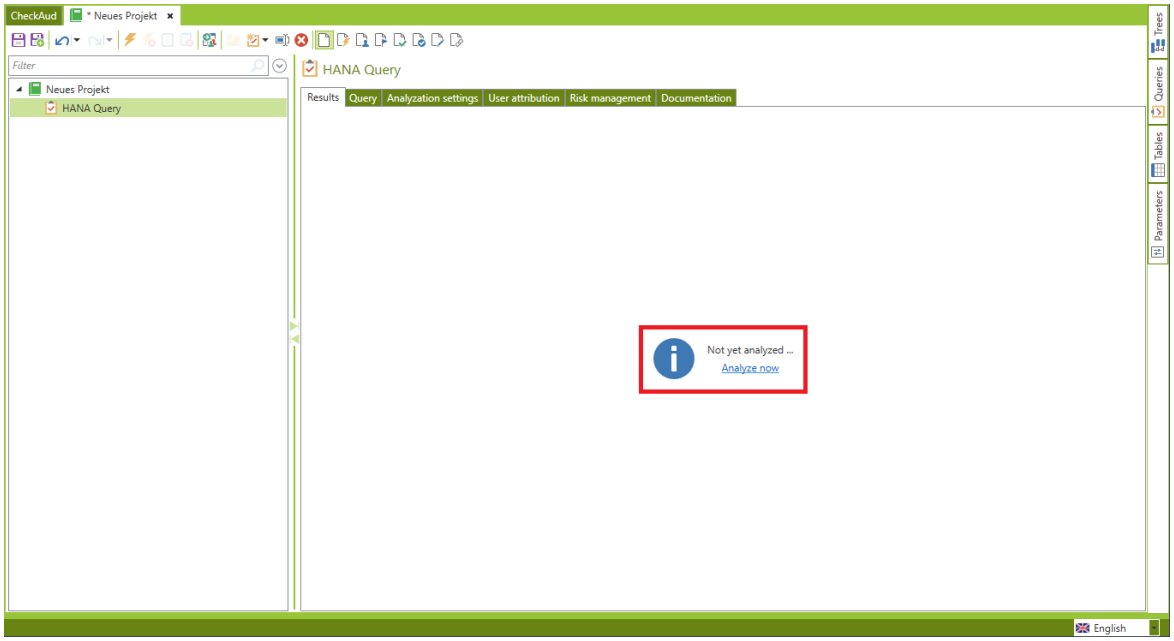



**Figure 114 - Evaluating an authorization query**

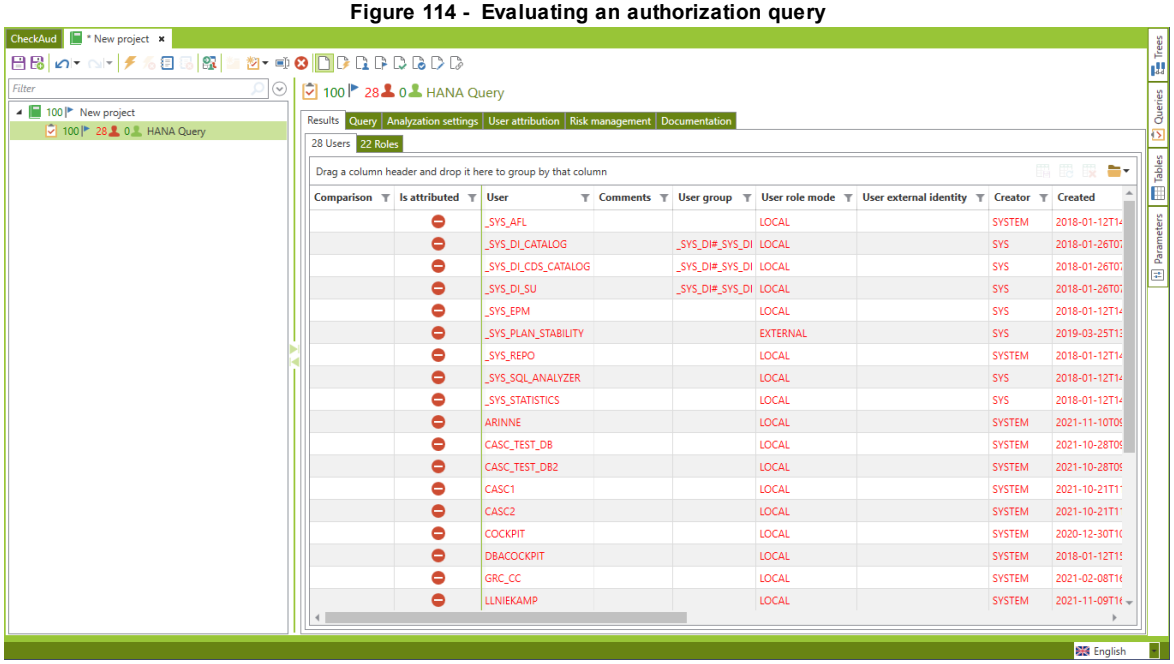



**Figure 115 - An evaluated authorization query**

Alternatively, the selected authorization query can be evaluated by choosing the button and the evaluation can be stopped by choosing the button.

Evaluated authorization queries are shown through the key figures in the results:

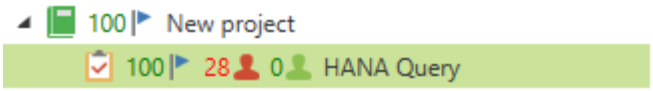
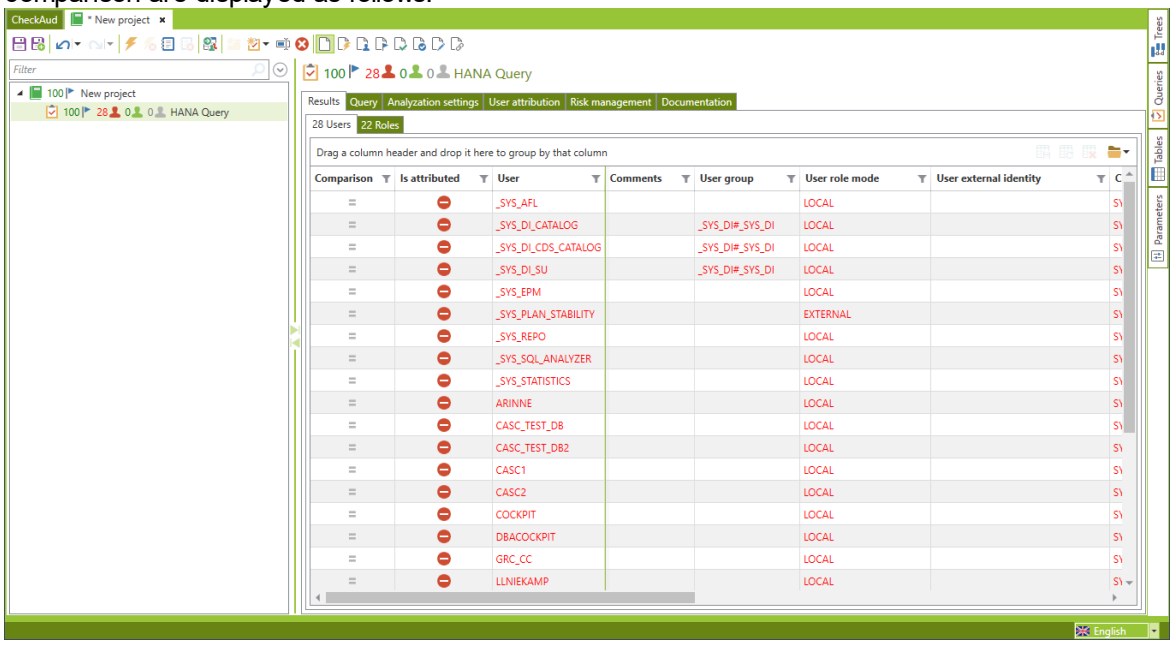



**Figure 116 - An evaluated authorization query**

If an additional snapshot was selected for comparison for the evaluation, the results of the comparison are displayed as follows:



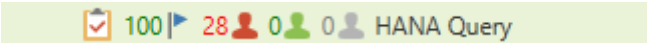




**Figure 117 - Evaluated authorization query, comparison of two snapshots**

Detailed information about the displayed results can be found in the chapter *Results Displayed in the Analysis Project*.

## III - 3.3 Evaluating a table query

To evaluate an individual table query, you must select it in the project. You can then start the evaluation for this table query using the *Analyze now* button on the *Results* tab.

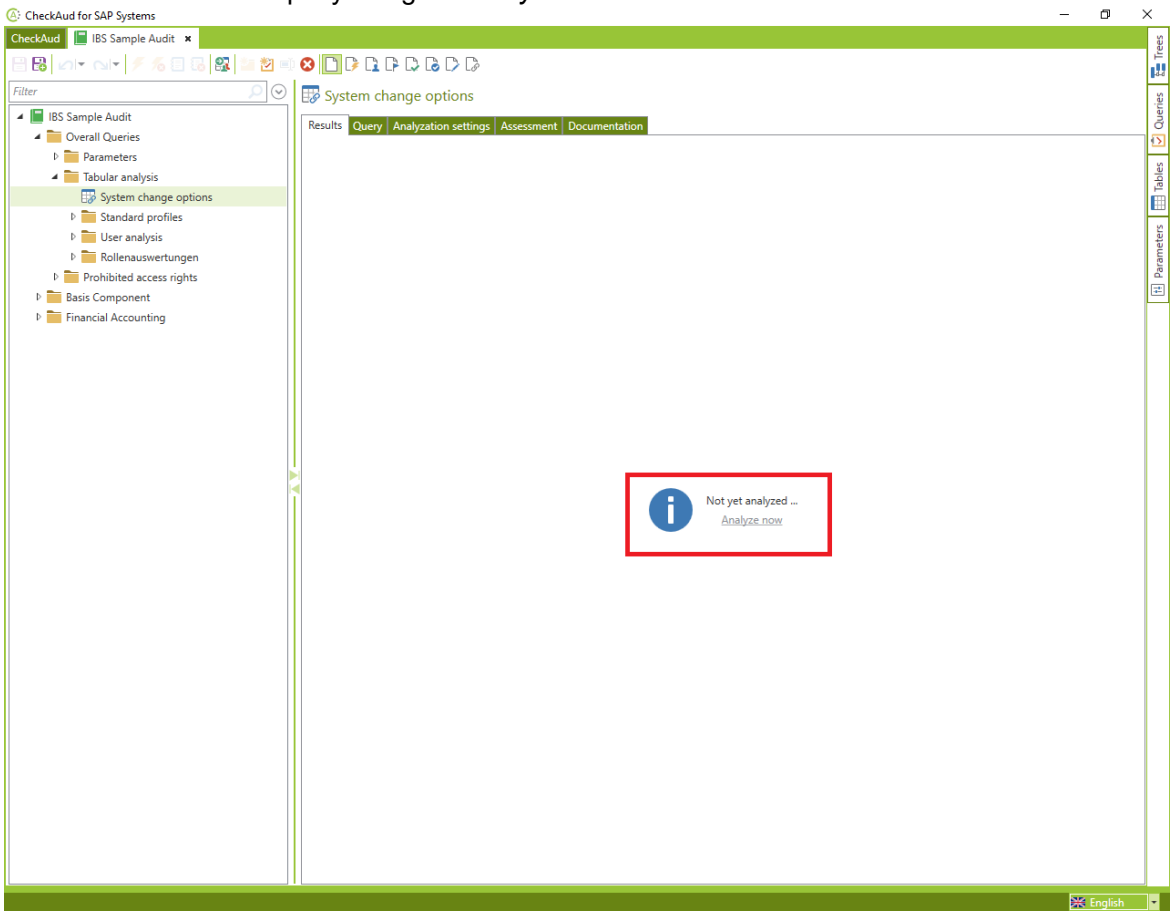



**Figure 118 - Evaluating a table query**

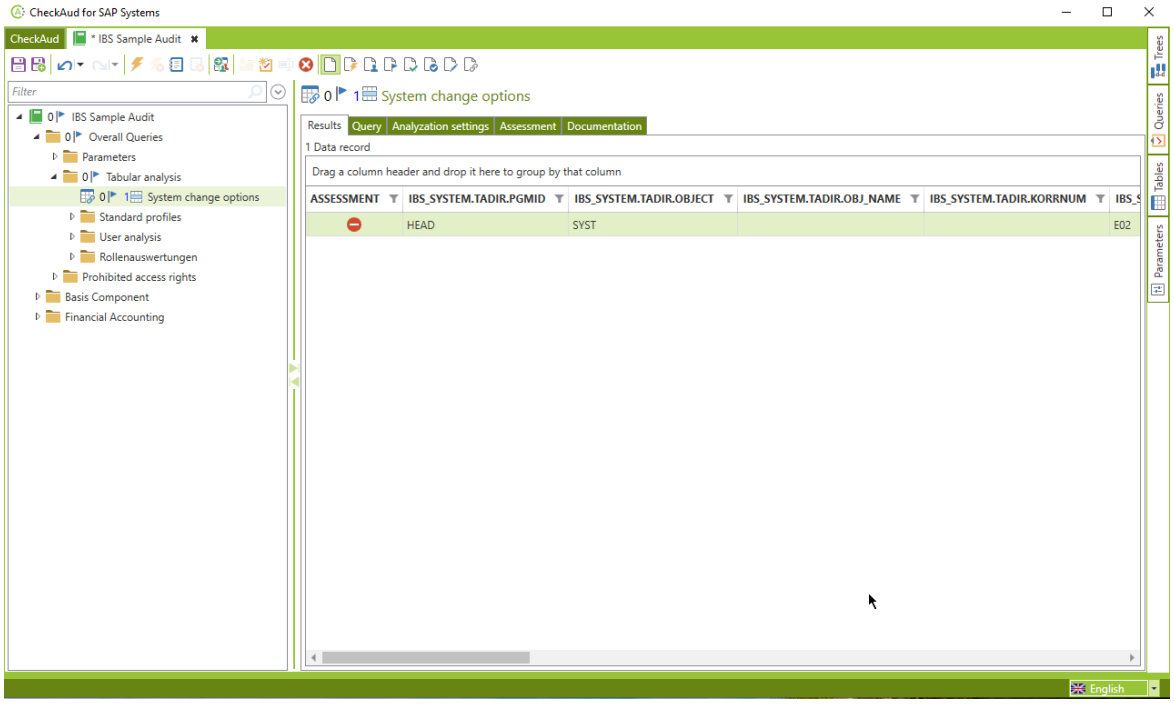



**Figure 119 - An evaluated table query**

Alternatively, the selected table query can be evaluated by choosing the button and the evaluation can be stopped by choosing the button.

Evaluated table queries are shown through the key figures in the results:

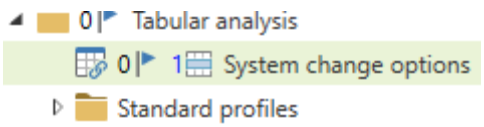



**Figure 120 - An evaluated table query**

Detailed information about the displayed results can be found in the chapter *Results Displayed in the Analysis Project*.

**Note:** this procedure for tabular evaluation can be used for ABAP and HANA DB systems.

## III - 3.4 Evaluating a parameter query

To evaluate a parameter query, you must select it in the project. You can then start the evaluation for this parameter query using the *Analyze now* button on the *Results* tab.

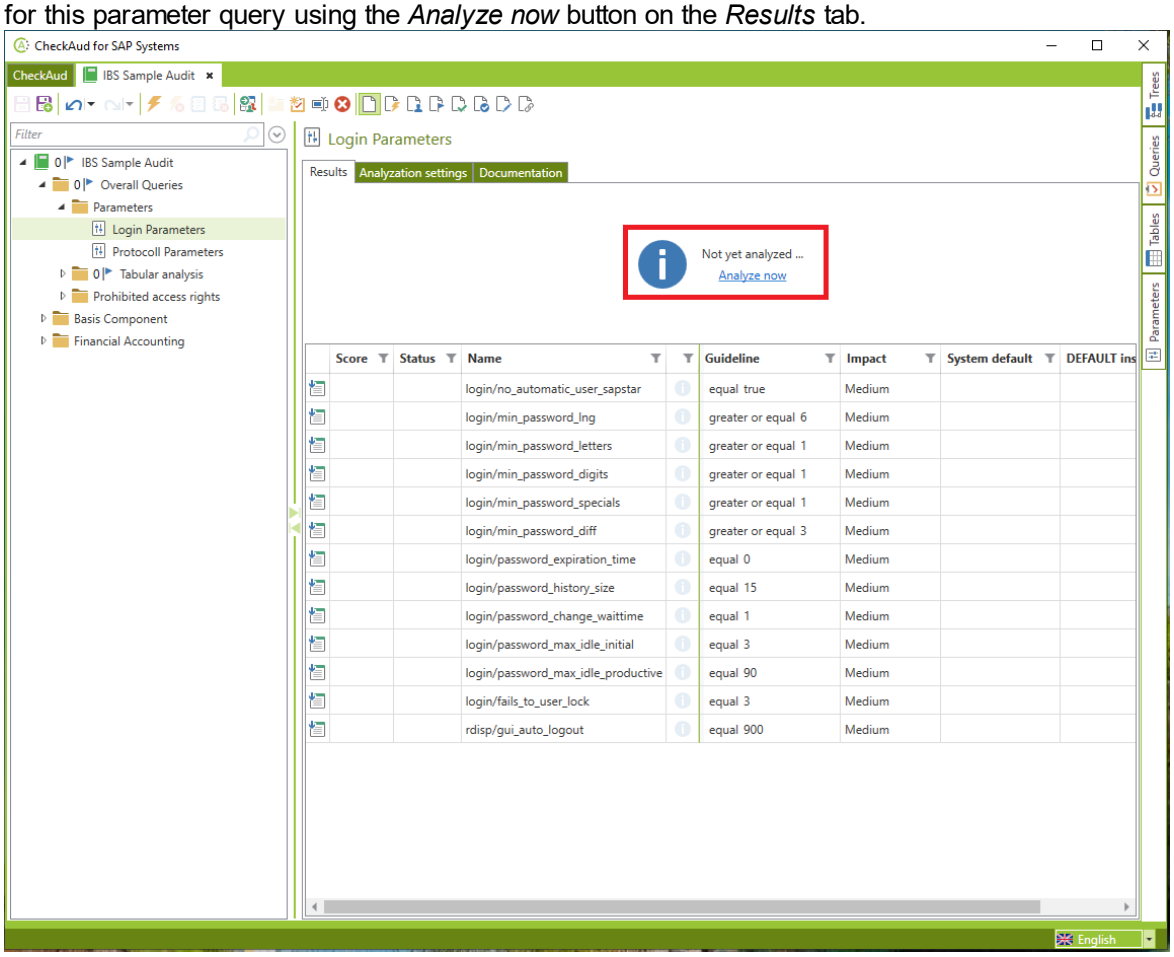



**Figure 121 - Evaluating a parameter query**

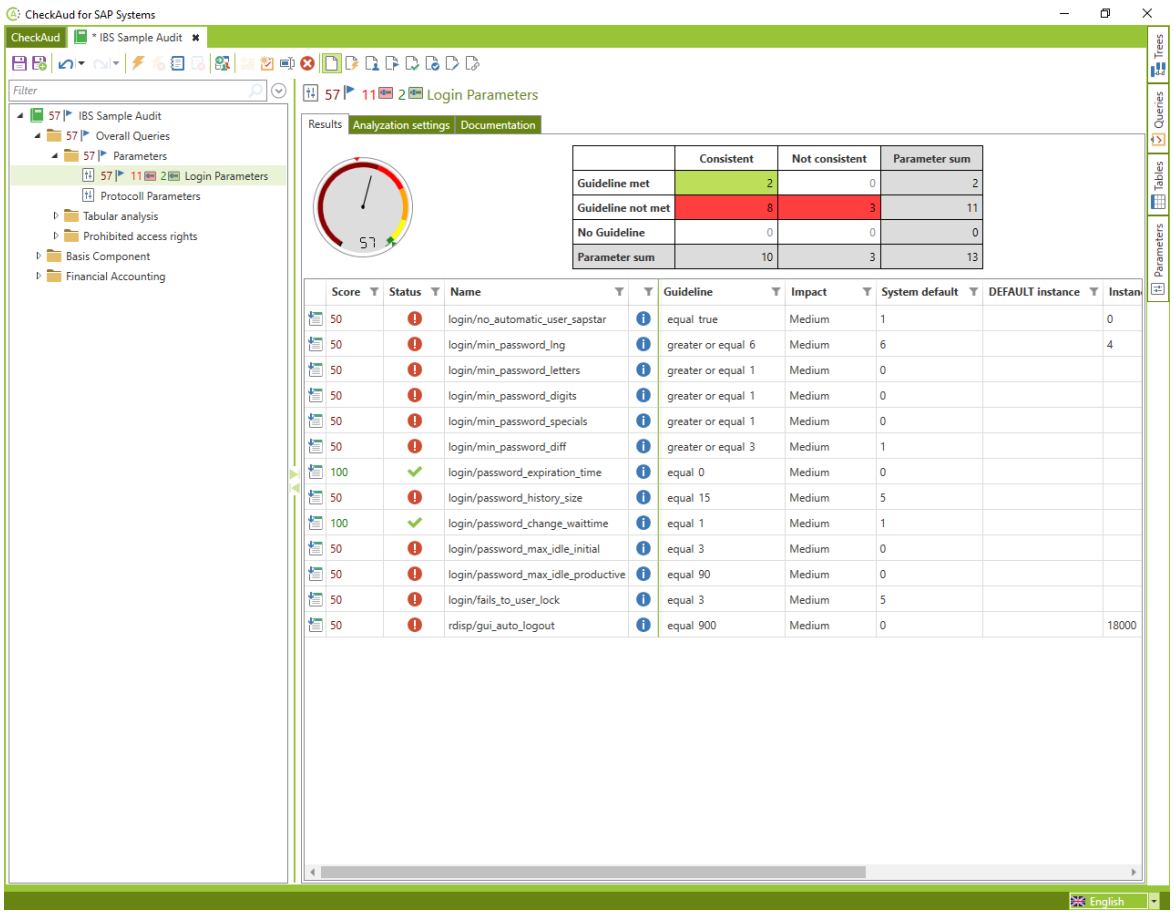



**Figure 122 - An evaluated parameter query**

Alternatively, the selected parameter query can be evaluated by choosing the button and the evaluation can be stopped by choosing the button.

Evaluated parameter queries are shown through the key figures in the results:

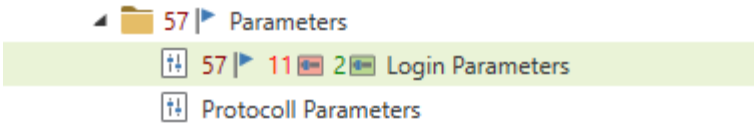



**Figure 123 - An evaluated parameter query**

Detailed information about the displayed results can be found in the chapter *Results Displayed in the Analysis Project*.

**Note**: The parameter values can be read out using the *Readout parameter values* option in CheckScan. (See the chapter *Reading Out Parameter Values*.)

**Note**: Parameters can be read out only from SAP systems with release level 7.40 or higher.

**Note:** for HANA DB systems there are currently no parameter evaluations available.

## III - 3.5 Evaluating multiple queries

To evaluate multiple queries within a subproject or within the overall analysis project, you must select the desired subproject or overall analysis project. You can use the and buttons to start and stop the overall analysis.

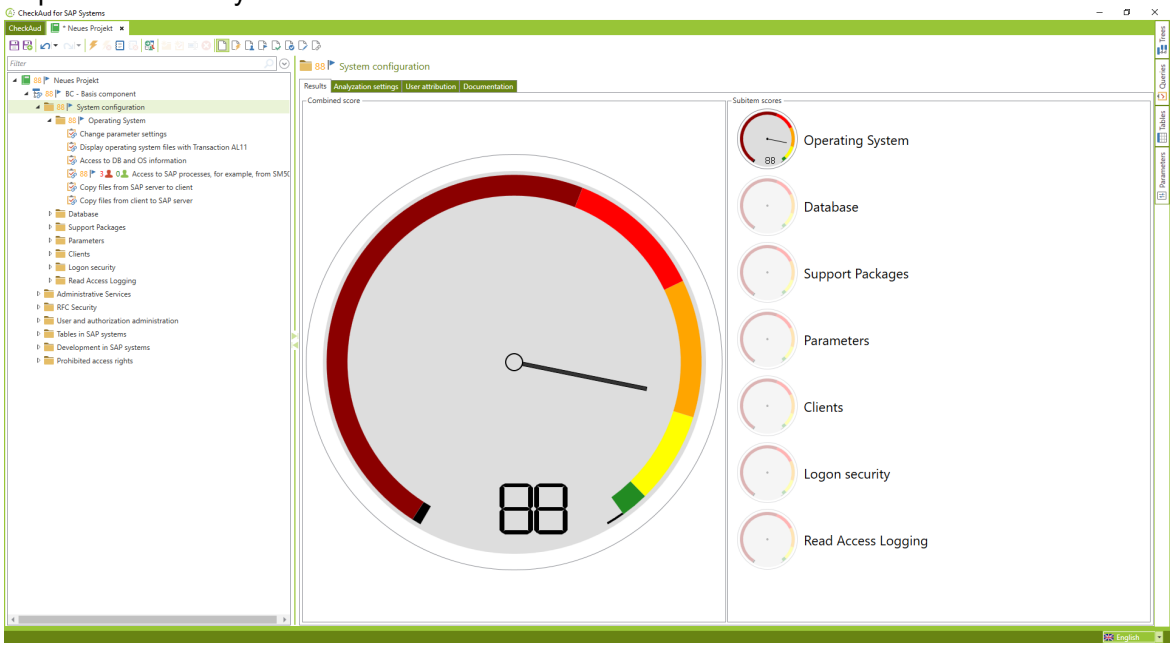



**Figure 124 - Overall evaluation of an analysis project**

The icon indicates that there are ongoing evaluations for the query in question.

# III - 4 Results display

The results of every query are displayed in a table. Depending on the query type, several options for optimizing the displayed results by sorting, filtering, grouping, showing and hiding information are provided.

## III - 4.1 Results display for an authorization query (ABAP)

### III - 4.1.1 Authorized users tab

The following results window shows the standard table view for an authorization query for authorized SAP users:

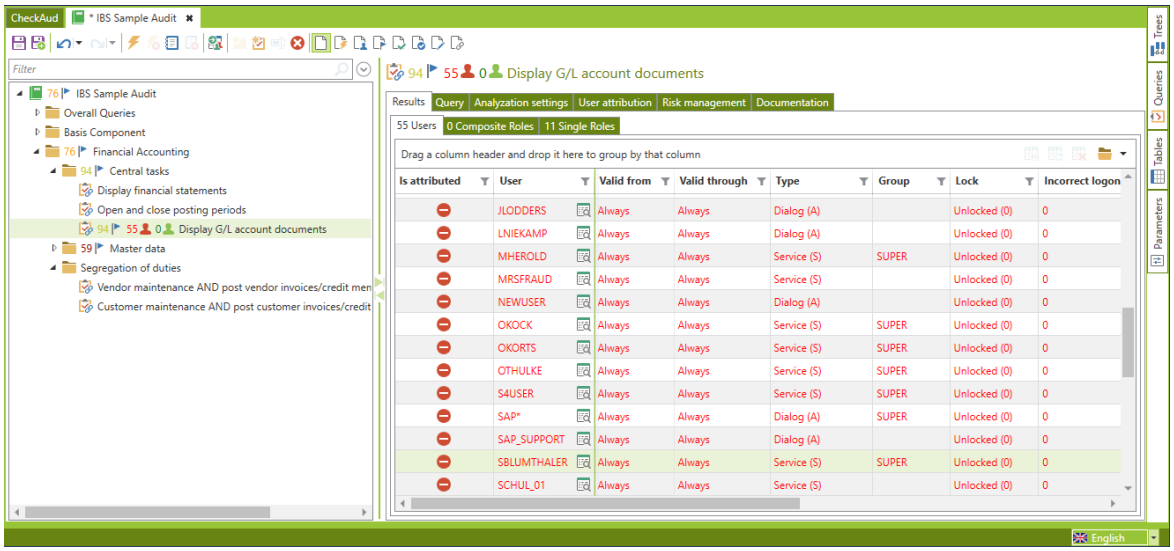



**Figure 125 - Authorization query table view: Authorized users**

In the table, you can display additional information for the columns by moving the mouse over the different fields.

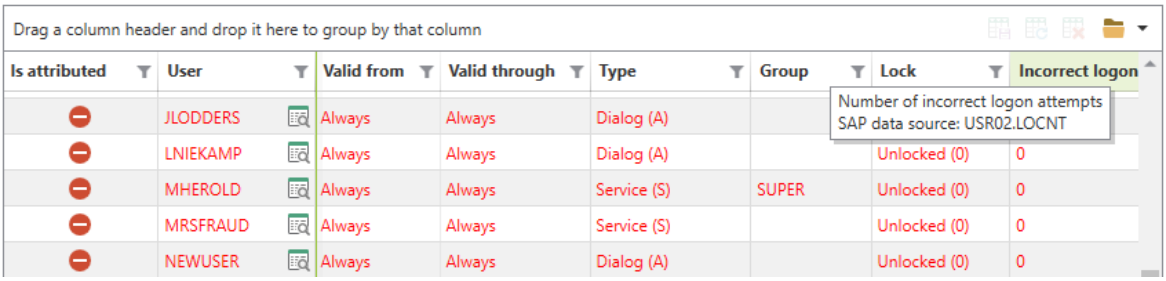



**Figure 126 - Detailed information about the columns**

By default, the query result is displayed only as a table. To display the origin of the authorization objects contained in the query for any user in the table, click the table line for the user in question to open a details window containing the authorization origins in the lower area:

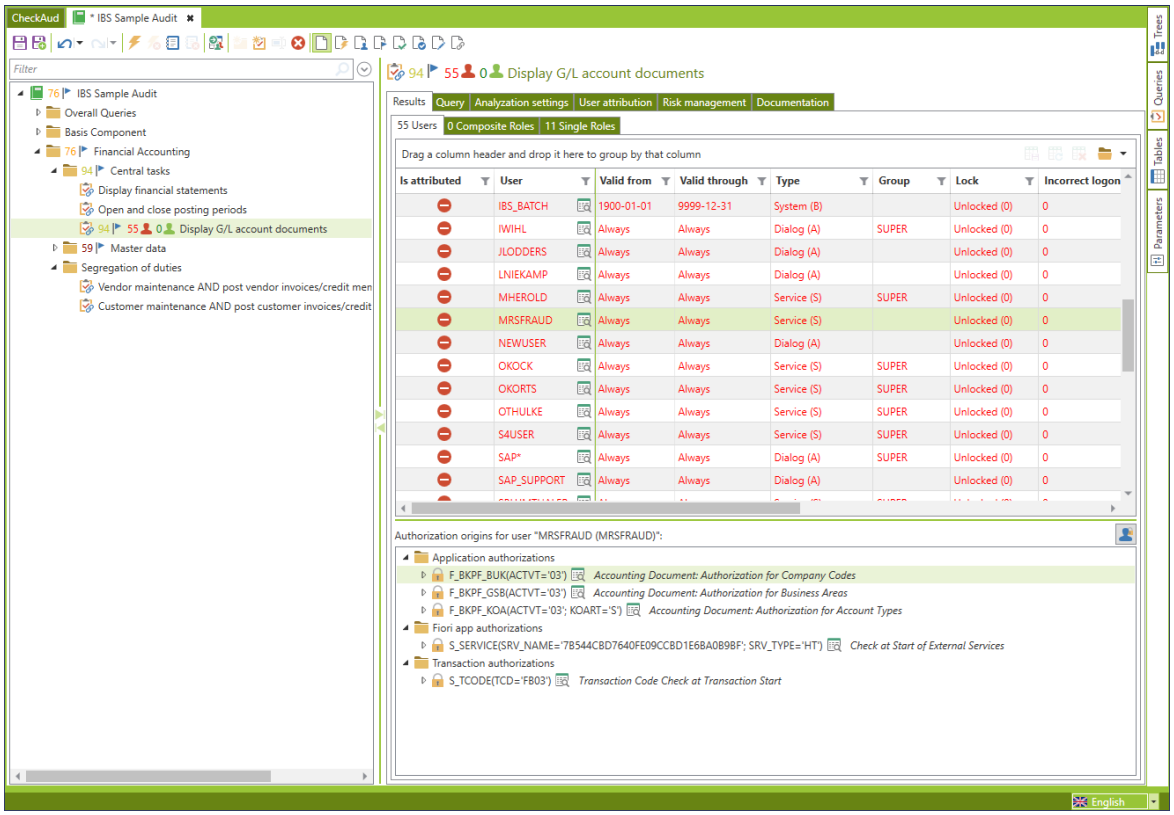



**Figure 127 - Result display including authorization origins for a selected user**

By default, the origins of application authorizations, Fiori app authorizations and transaction authorizations are displayed separately. First the queried authorization object is shown, including the queried field values.

The corresponding long texts are shown alongside the overview of the objects, roles, profiles and users.

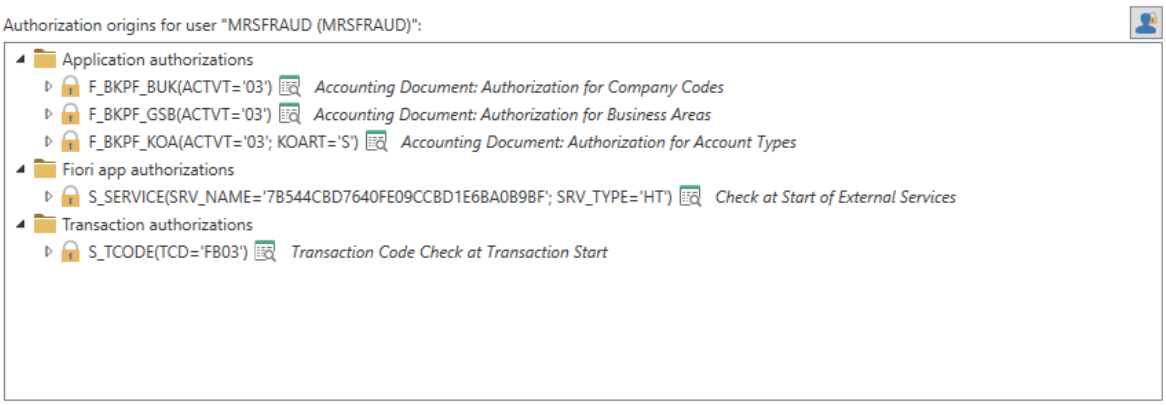



**Figure 128 - List of application- Fiori app- and/or transaction authorizations**

Expand the tree to see the full list of that user's authorizations and their origins:

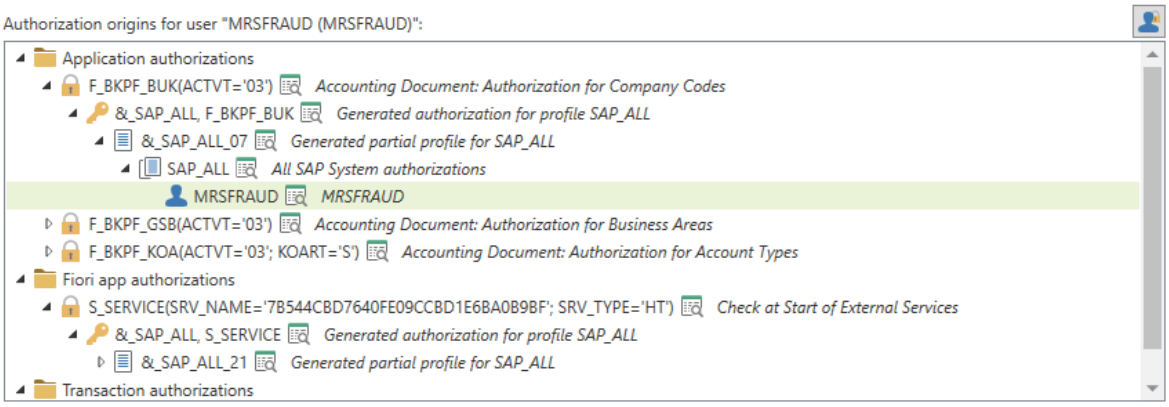



**Figure 129 - Origin and value of an authorization object**

The following symbols are used to represent authorization origins:

| | |
|---|---|
| | Authorization object in the query (including the field value) |
| | Technical authorization in the SAP system |
| | Generated profile |
| | SAP single role |
| | SAP composite role |
| | SAP standard single profile |
| | SAP standard composite profile |
| | Reference user |
| | Display the technical details for the selected element |

As an alternative to the standard display of authorization origins subdivided into application and transaction authorizations, the button can be used to switch to the view of the participating roles:

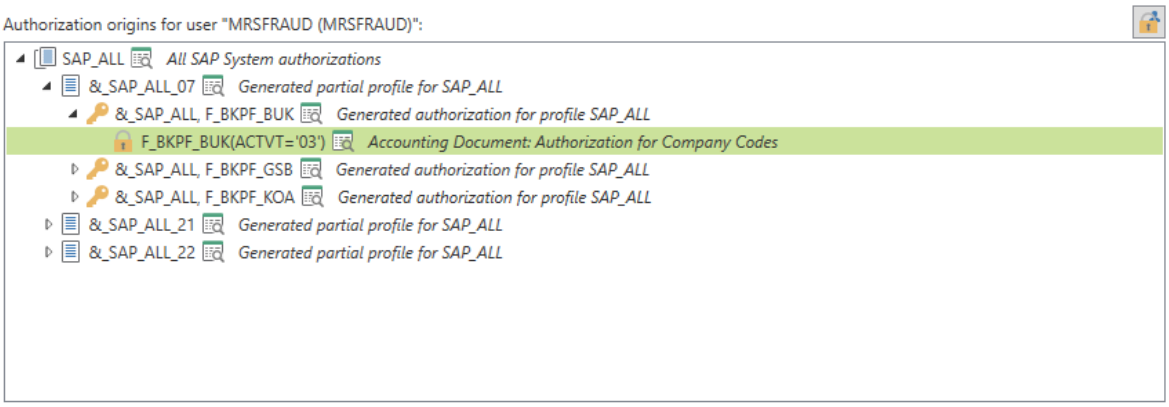



**Figure 130 - Authorization origin of a user from the view of the participating roles**

The results are displayed in short form in the analysis project:


**1 2 3 4 5**

1 - Symbol for calculated query incl. color-coding according to score
2 - Calculated score (0 = low system security and 100 = high system security)
3 - Number of technically authorized users (not legitimized according to target specification)
4 - Number of technically authorized users (legitimized according to target specification)
5 - Name of the query

### III - 4.1.2 Authorized users tab compairing snapshots

If you have selected a second snapshot for comparison in the analysis settings, the results of the comparison are displayed as follows. In the User tab, the results window also includes a “Comparison” column:

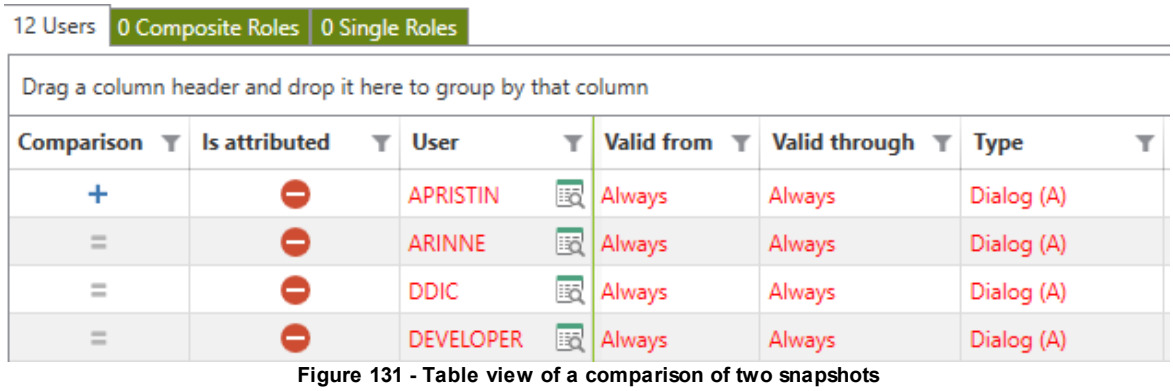



**Figure 131 - Table view of a comparison of two snapshots**

The following symbols are used to display the results of a comparison of two snapshots:

| | |
|---|---|
|  | The user is no longer included in the current snapshot |
|  | Newly authorized: The user is newly authorized for the authorization query under inspection in the current snapshot |
|  | Previously authorized: The user is no longer authorized for the authorization query under inspection in the current snapshot |
|  | Unchanged: The user is authorized for the authorization query under inspection in both the current snapshot and the snapshot for the comparison |

The results are displayed in short form in the analysis project:


6 - Number of technically authorized users who were newly authorized
7 - Number of technically authorized users who were previously authorized

If the snapshots to be compared have different SAP system release levels or changed Customizing settings, the authorization query in question may be evaluated with a different definition. This is the case for release-independent authorization queries (authorization queries that are evaluated with different object compositions/definitions based on the SAP system release). For more information, see the chapter *Release-Independent Authorization Queries*. Such a case is indicated with a message in the displayed results:

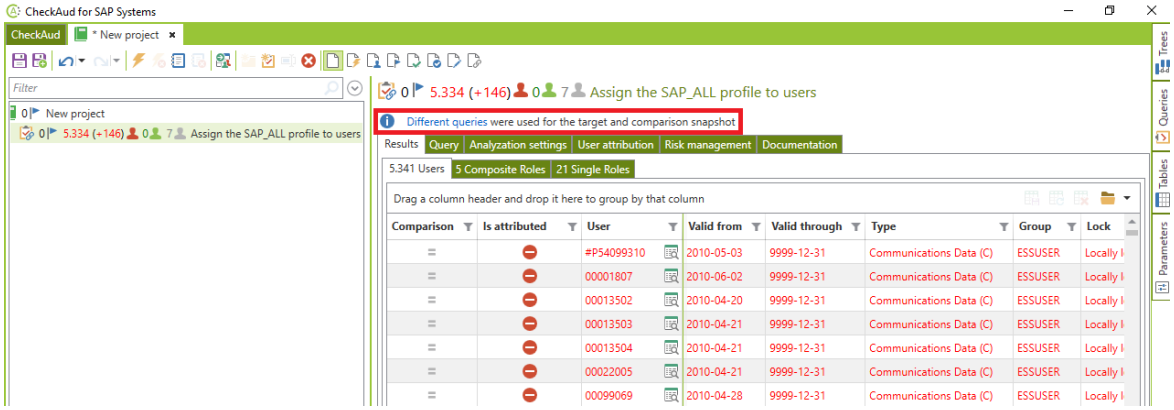



**Figure 132 - Message indicating a different query composition in the comparison**

The differences in the query used for the snapshot can be displayed by clicking the *Different queries link*

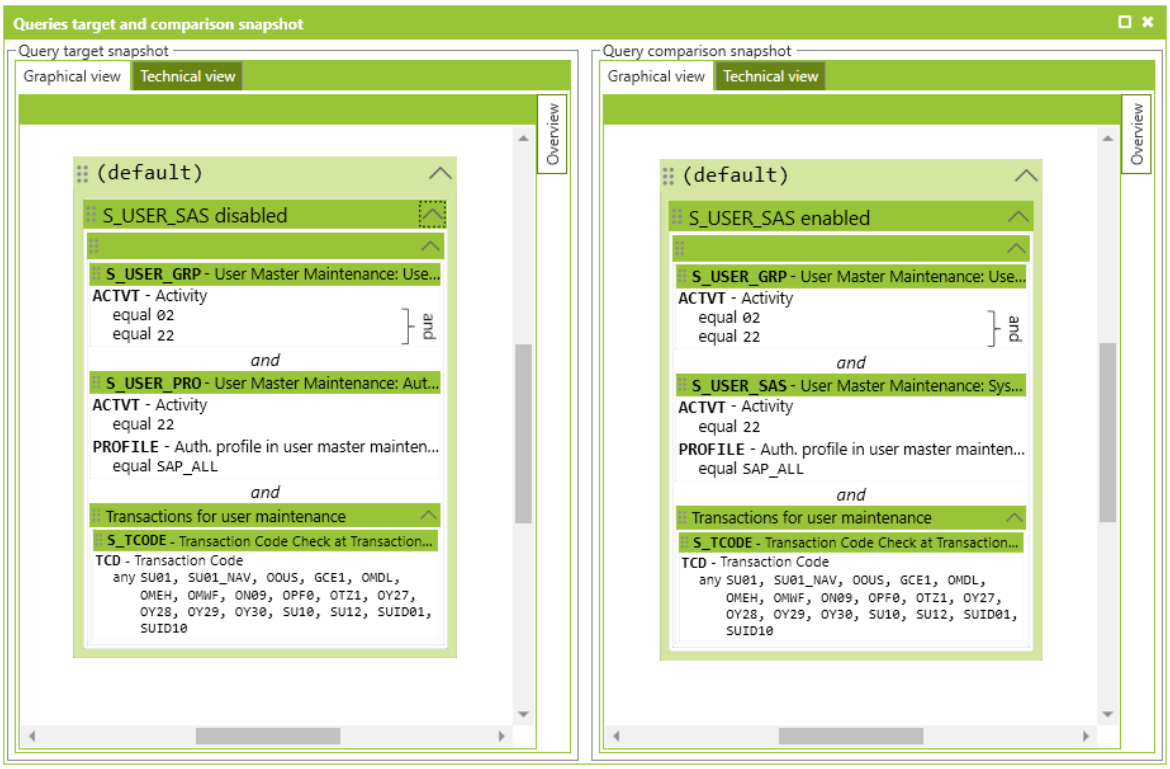



**Figure 133 - Message indicating a different query composition in the comparison**

### III - 4.1.3 Authorized composite roles tab

Use the *Composite roles* tab to create a table displaying the group roles that fully include the queried authorization, regardless of whether the role is assigned to any users:

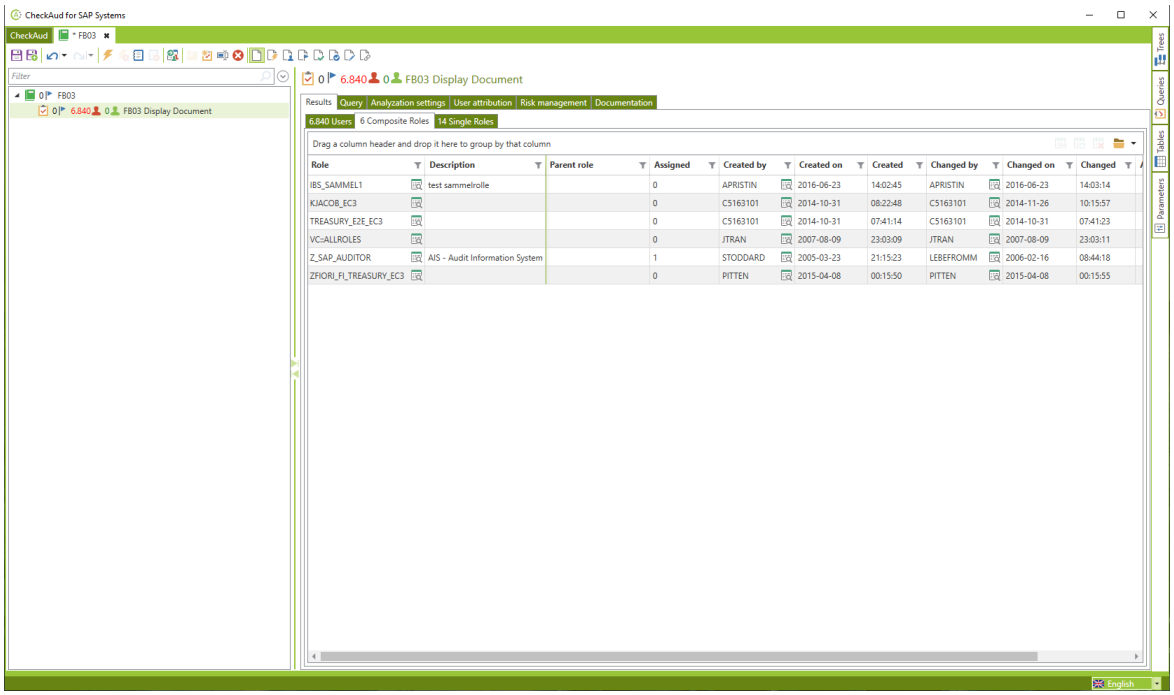



**Figure 134 - Authorization query table view: Authorized composite roles**

When you select an individual composite role, you can display the origins of the authorizations for this selected composite role.

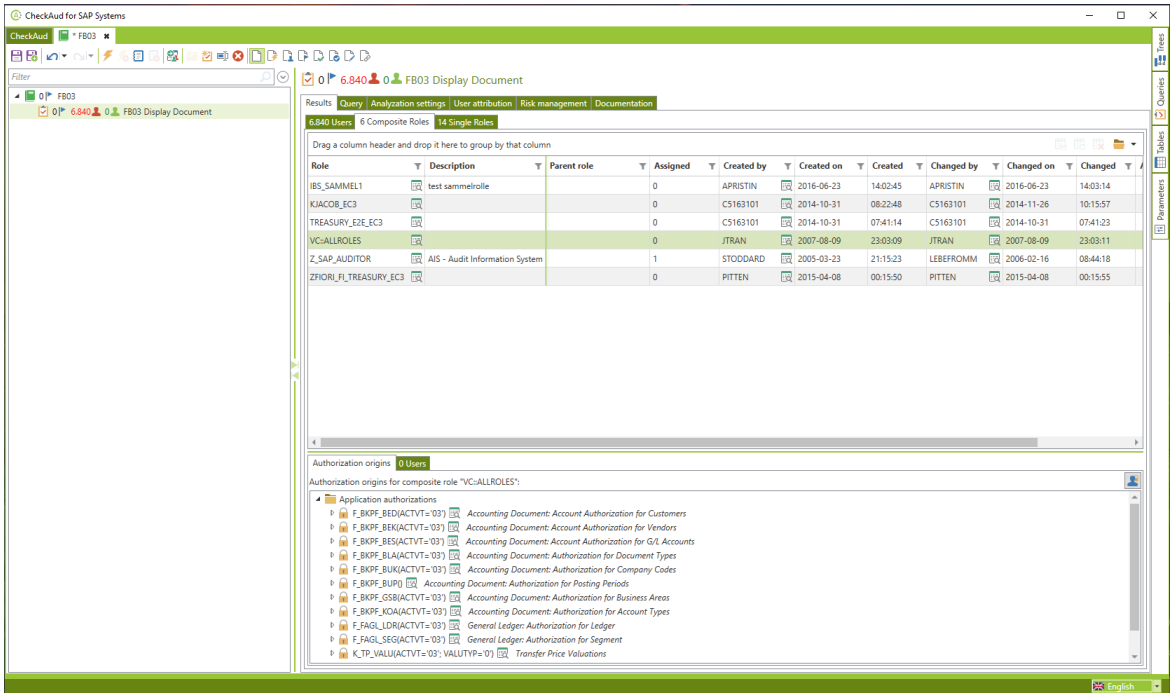



**Figure 135 - Origins of the authorizations of a composite role**

By default, the origins of application authorizations and transaction authorizations are displayed separately. First the queried authorization object is shown, including the queried field values.

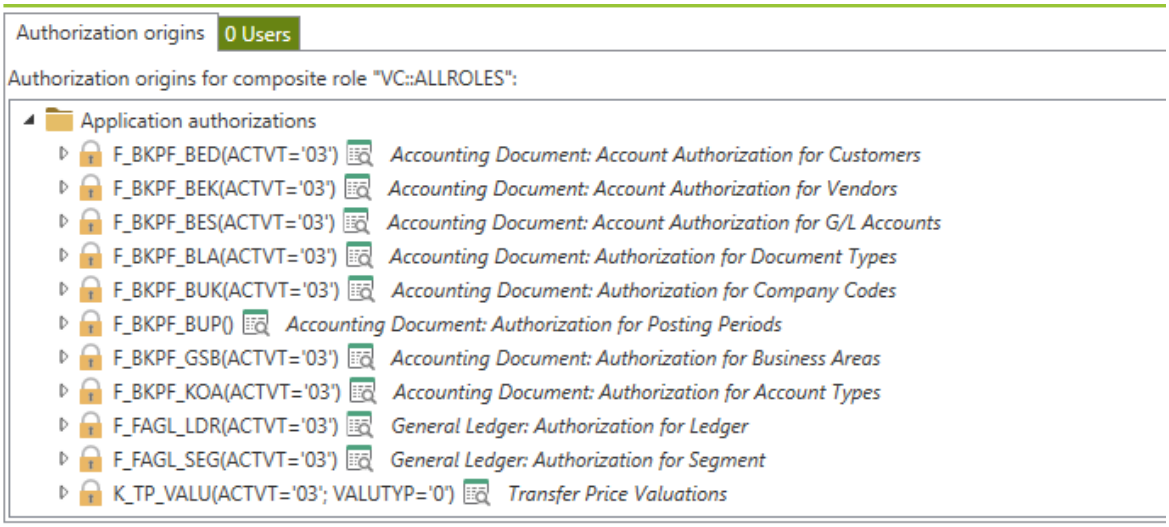



**Figure 136 - List of application and/or transaction authorizations in a composite role**

Select the *Users* tab to list all the users defined in the composite role.

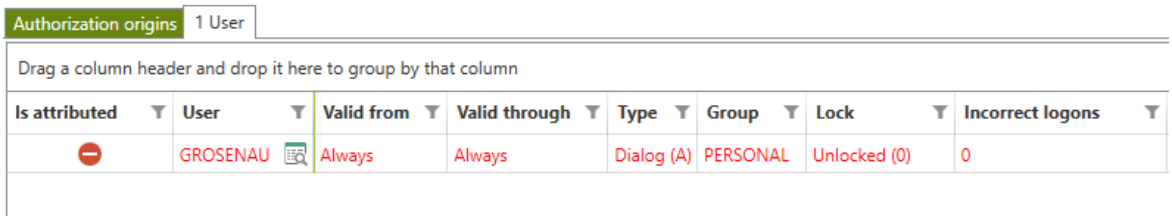



**Figure 137 - Users assigned to the composite role**

You can display the role assignment path of the individual users by selecting the user in question.

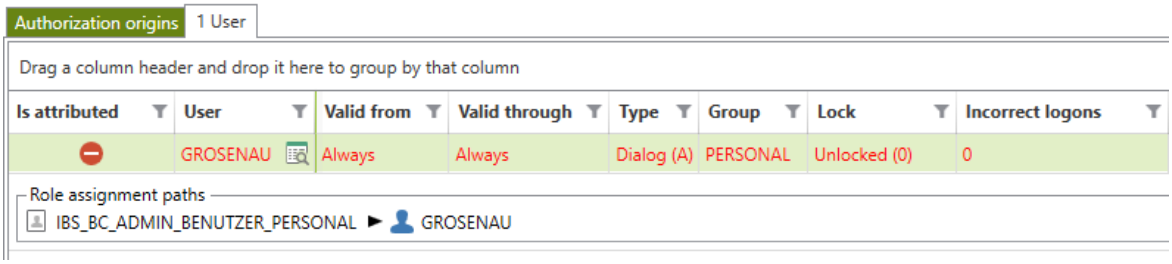



**Figure 138 - Role assignment path of the user**

### III - 4.1.4 Authorized single roles tab

Use the *Single roles* tab to create a table displaying the individual roles that fully include the queried authorization, regardless of whether the role is assigned to any users:

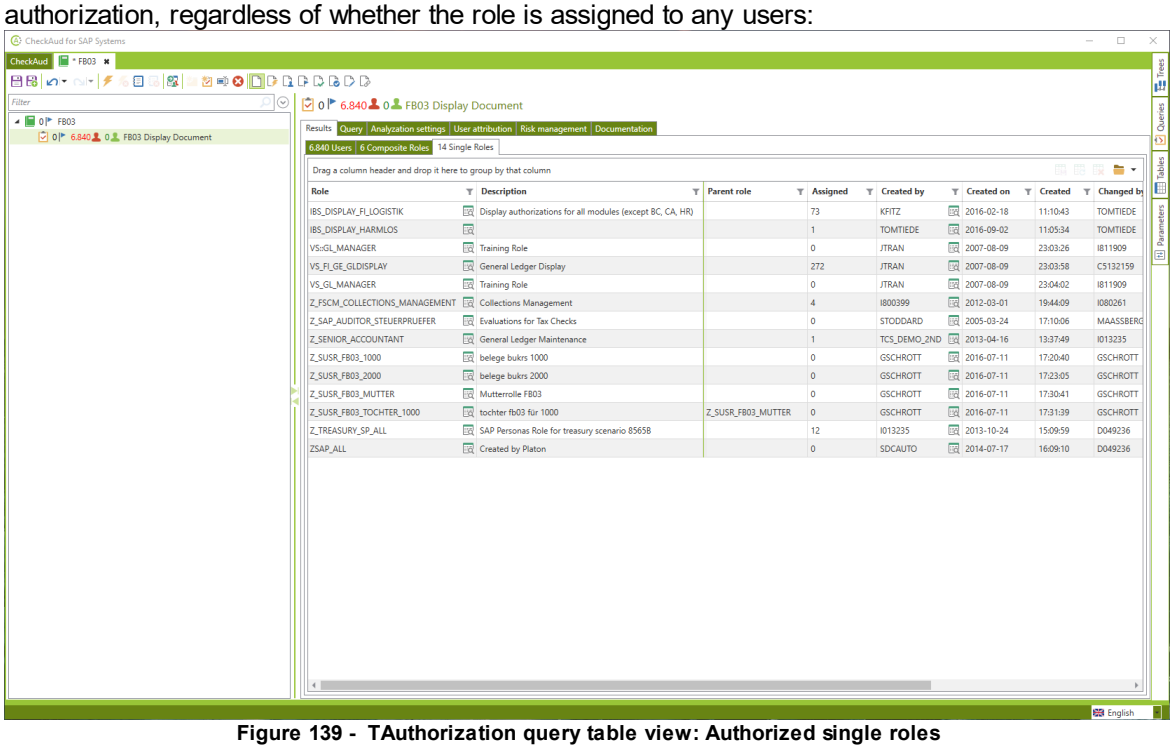



**Figure 139 - TAuthorization query table view: Authorized single roles**

When you select a single role, you can display the origins of the authorizations for this selected single role.

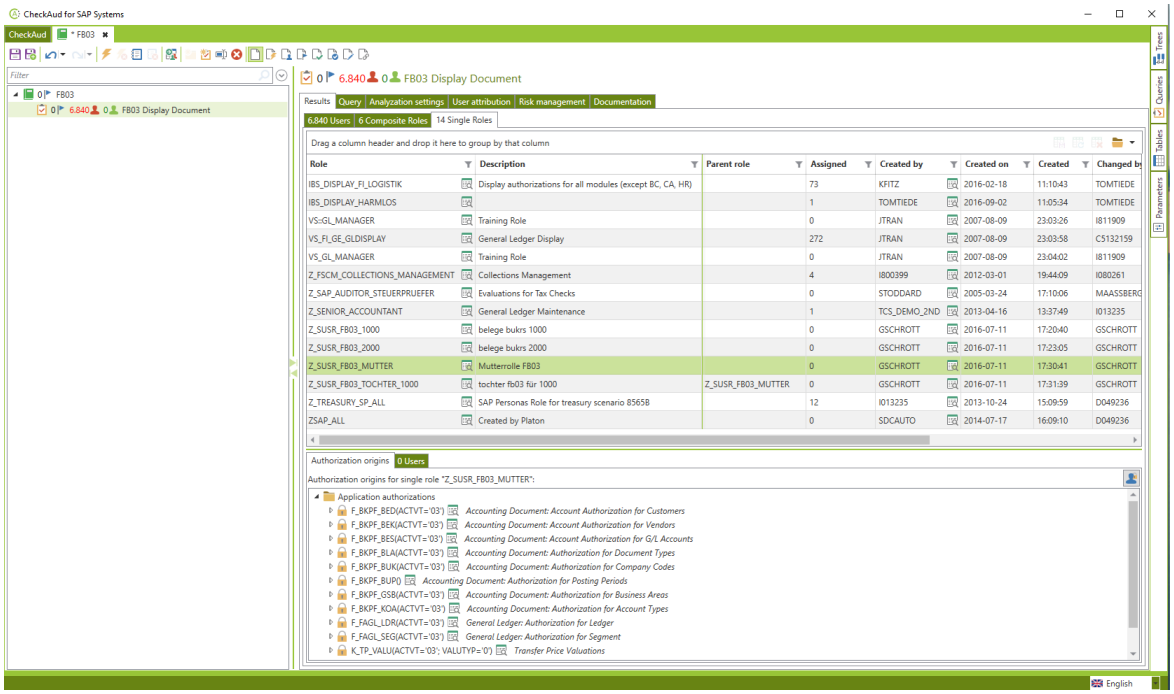



**Figure 140 - Origins of the authorizations of an single role**

By default, the origins of application authorizations and transaction authorizations are displayed separately. First the queried authorization object is shown, including the queried field values.

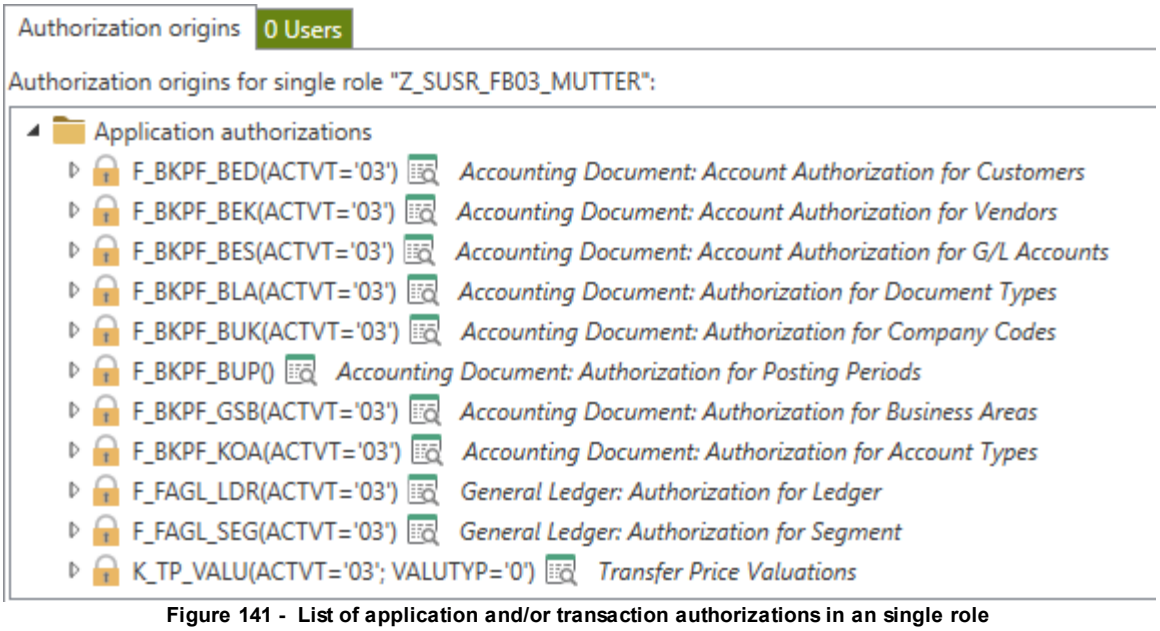



**Figure 141 - List of application and/or transaction authorizations in an single role**

Select the Users (Benutzer) tab to list all the users defined in the single role.

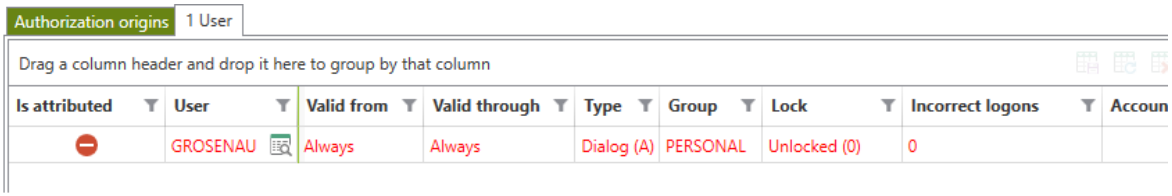



**Figure 142 - Users assigned to the single role**

You can display the role assignment path of the individual users by selecting the user in question.

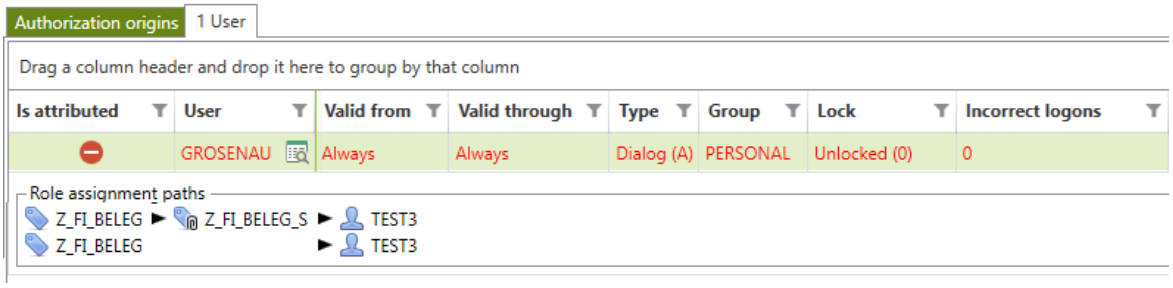



**Figure 143 - Role assignment path of the user**

### III - 4.1.5 Details window

The details window lets you display the authorization values of users, roles and profiles in a simple way.

Click the  icon to display information about:

- Queried authorization objects
- Authorizations
- Individual and composite profiles
- Individual and composite roles
- Reference users
- Users.

For HANA evaluations:

- Queried Privileges.
- Repository, catalog, and HDI roles
- Users
- Schema objects
- Repository packages.

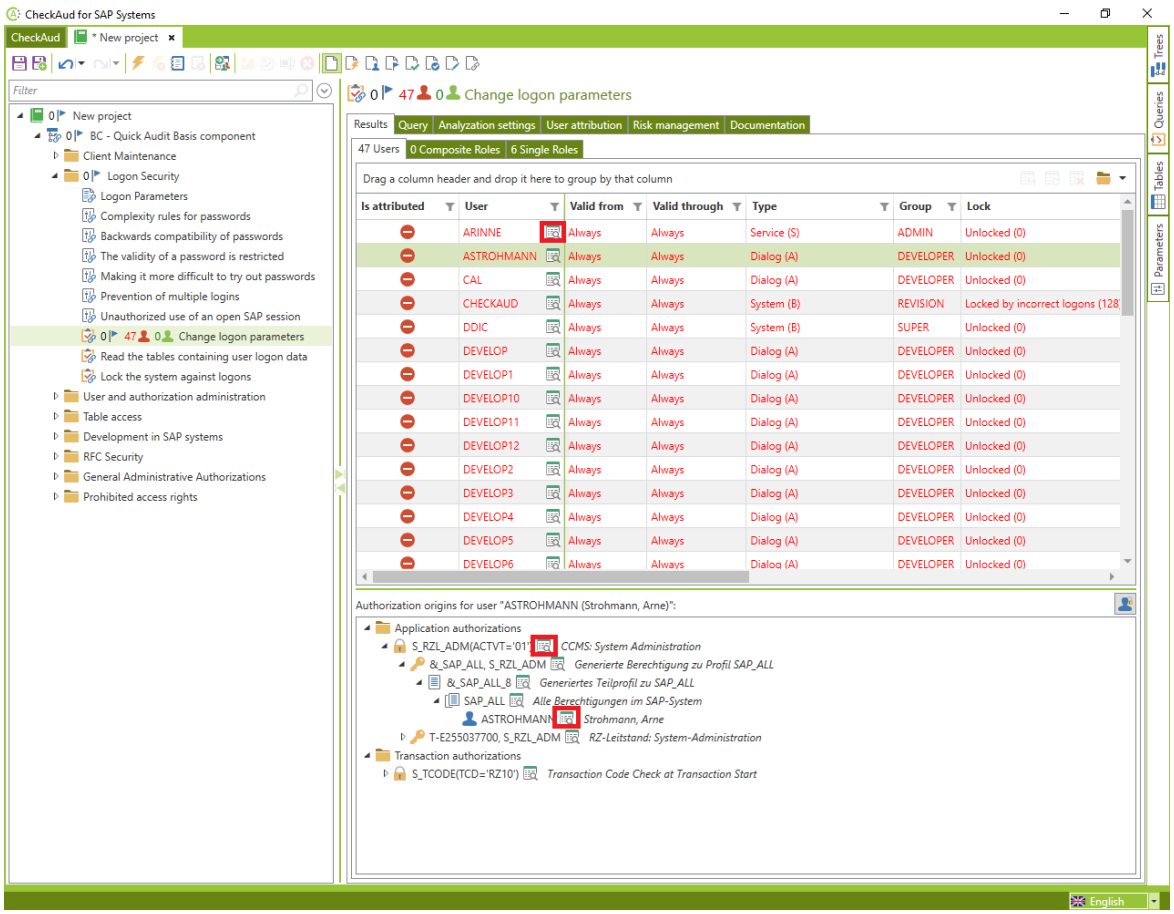



**Figure 144 - Accessible details window**

The example below shows a details window for an single role:

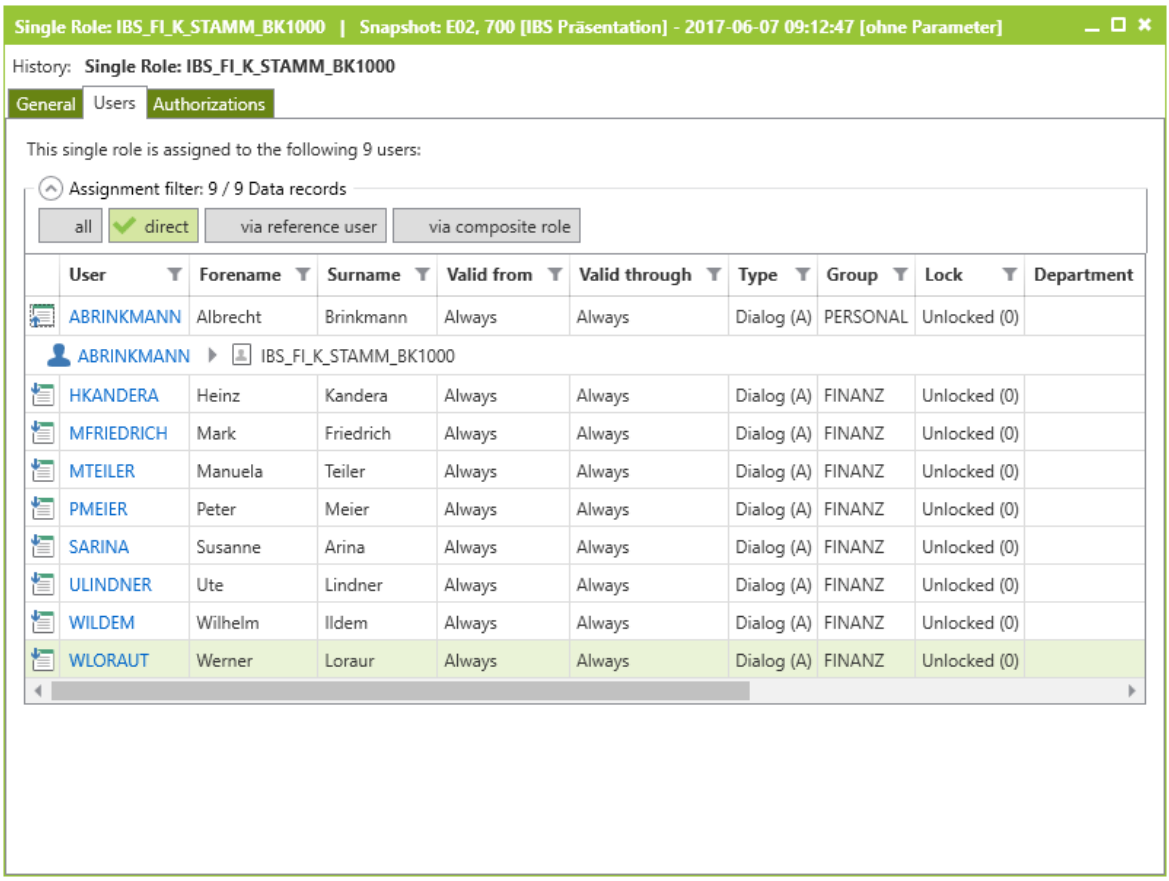



**Figure 145 - Example of a details window**

The information shown and its arrangement depend on the details window selected. Basic information is shown in all windows if it is available.

1 - Window information: The window information shows which role, user, profile or similar of the examined snapshot the information currently displayed belongs to.
2 - Tab pages: Tab pages allow you to display various types of information about your selection.
3 - History: Fields with blue text allow the associated object to be displayed in its own details view. A history is kept starting with the first details window called up. Thus it is possible to retrace your steps, and you can jump back to the previous information or even to the very first details window opened at any time.
4 - Assignment filter: The assignment filter allows the displayed information to be filtered by various criteria.
5 - Ad hoc filter for the table view: the filter provides a number of different filter modes. (For more information, see the chapter *Custom Layouts for the Table Display*.)

6 - Expanding information: You can use the and buttons to display and hide additional information.

### III - 4.1.6 Details window - Authorization

Tab page: *General*

The *General* tab page contains information on the authorization and the authorization object. The single role / single profiles in which the authorization can be found are listed on the right-hand side of the details window. Click on the object with blue text to navigate to the corresponding details window.

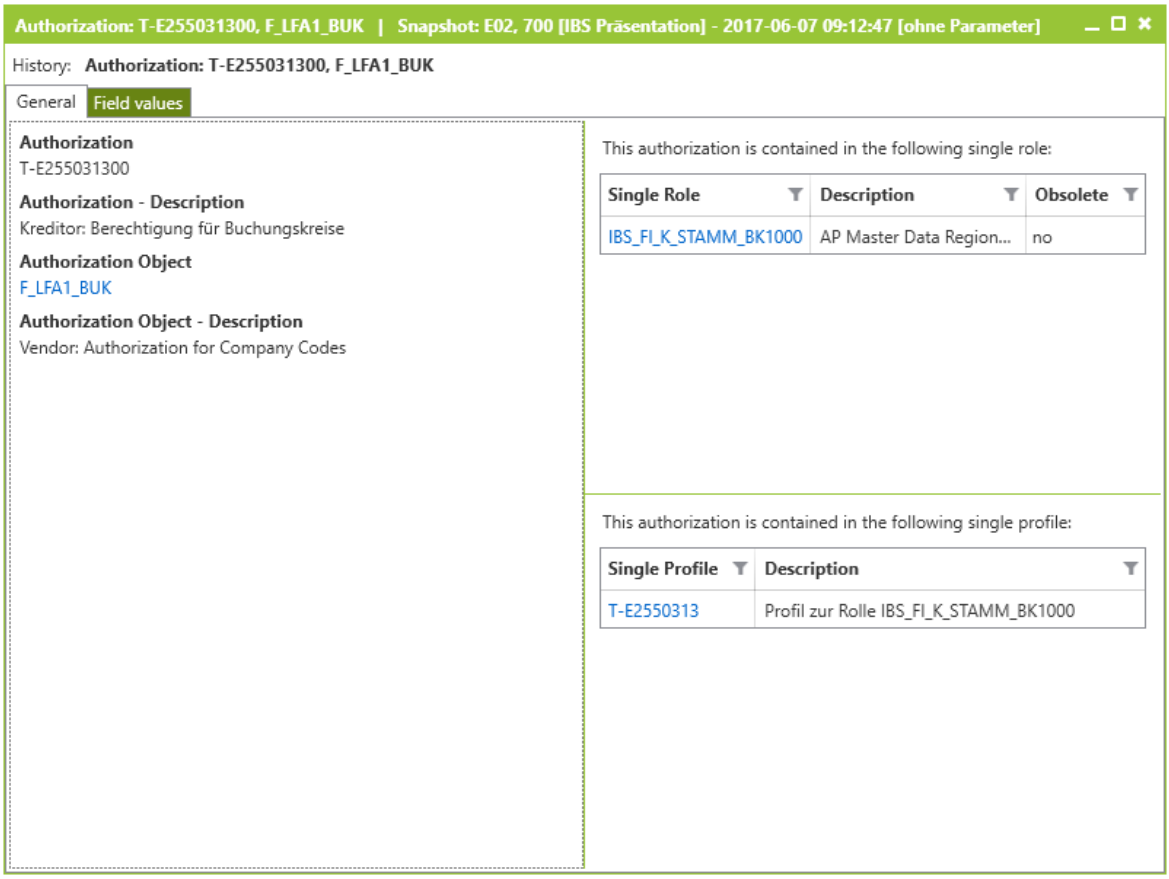



**Figure 146 - Authorization details window**

Tab page: *Field values*

The *Field values* tab page shows the fields and field values belonging to the authorization.

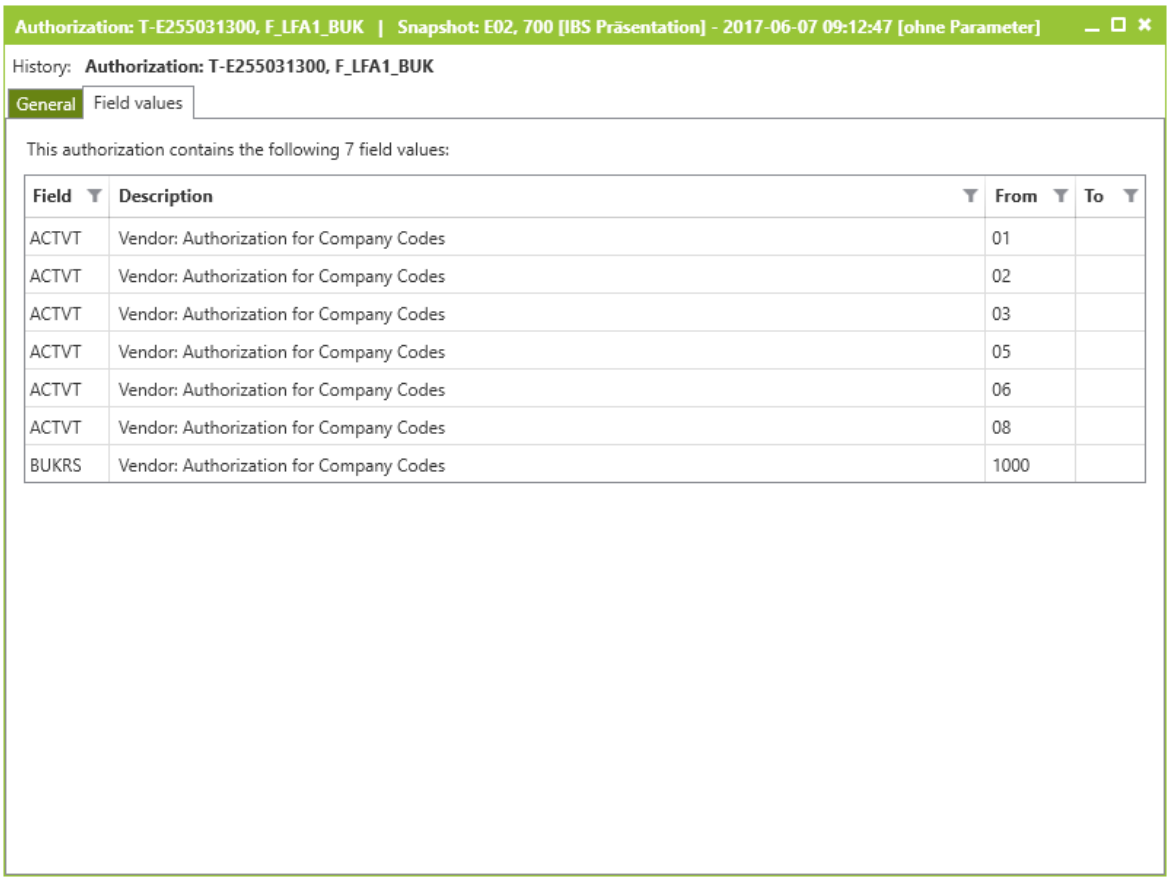



**Figure 147 - Authorization details window**

### III - 4.1.7 Details window - Single profile

Tab page: *General and authorizations*

The *General and authorizations* tab page shows information on the single profile and the authorizations contained in it as well as their descriptions. Click on the object with blue text to navigate to the corresponding details window.

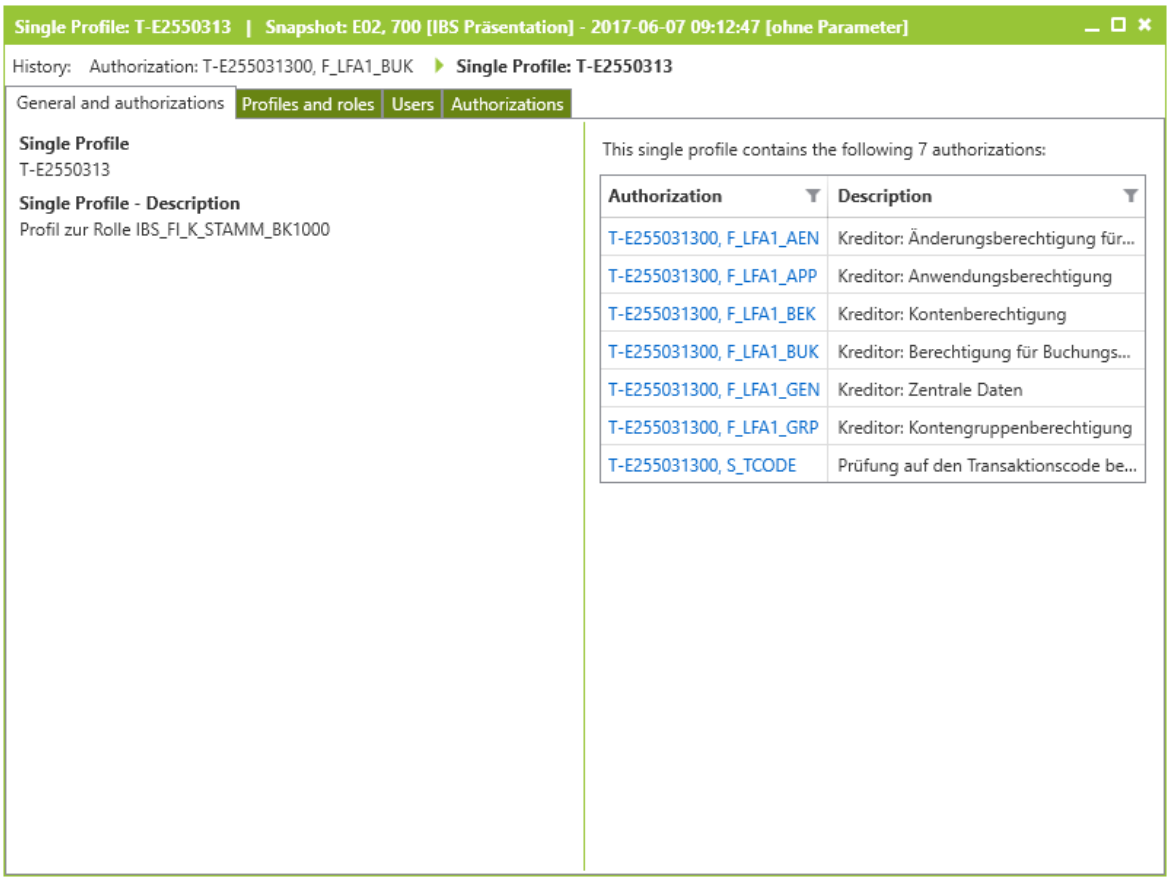



**Figure 148 - single profile details window (general and authorizations)**

Tab page: *Profiles and roles*

The Profiles and roles (Profile und Rollen) tab page contains information about whether the individual profile is contained in composite profiles. The assignment filter allows filtering of the composite profiles based on the following criteria: All, Direct, via composite profile. In addition, it can be determined whether the single profile is contained in a single or composite role. Expand the composite role to see the paths with which the profile is contained in a composite role. Click on the object with blue text to navigate to the corresponding details window.

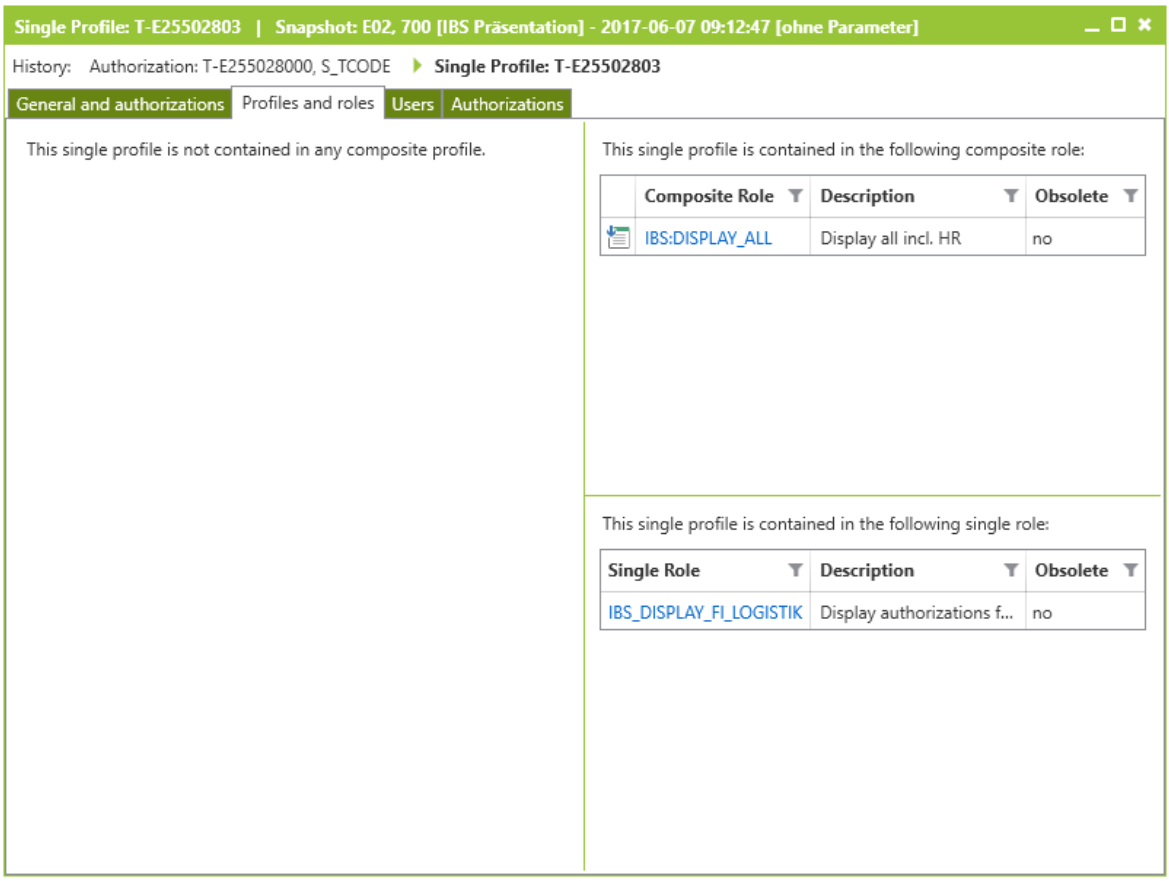
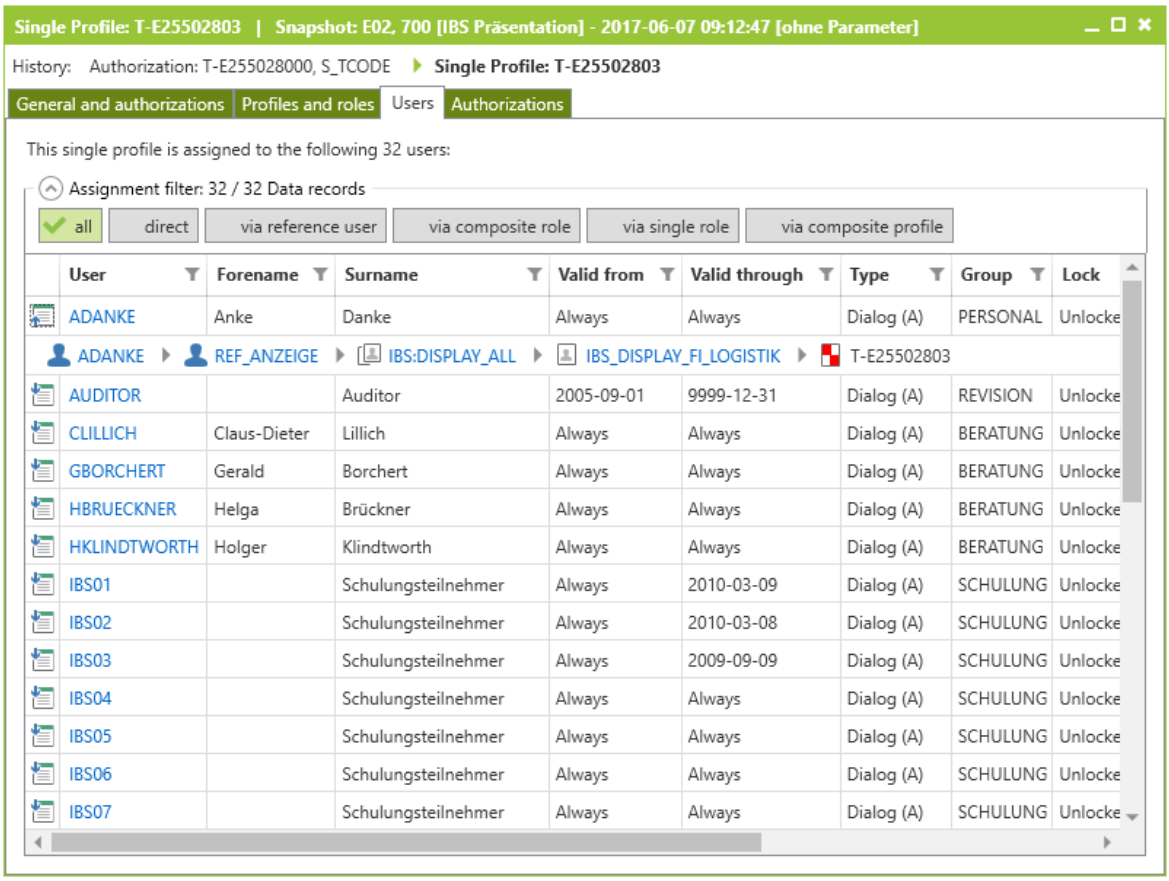



**Figure 149 - single profile details window (profiles and roles)**

Tab page: *Users*

The Users tab page lists all of the users assigned to the selected single role. The assignment filter allows filtering of the composite profiles based on the following criteria: All, Direct, via reference users, via composite role, via single role, via composite profile. Expand .a user to see the single role or composite role from which that user receives its profile, as well as the single roles and profiles it contains. Click on the object with blue text to navigate to the corresponding details window.




| User | Forename | Surname | Valid from | Valid through | Type | Group | Lock |
|---|---|---|---|---|---|---|---|
| ADANKE | Anke | Danke | Always | Always | Dialog (A) | PERSONAL | Unlocke |
| AUDITOR | | Auditor | 2005-09-01 | 9999-12-31 | Dialog (A) | REVISION | Unlocke |
| CLILLICH | Claus-Dieter | Lillich | Always | Always | Dialog (A) | BERATUNG | Unlocke |
| GBORCHERT | Gerald | Borchert | Always | Always | Dialog (A) | BERATUNG | Unlocke |
| HBRUECKNER | Helga | Brückner | Always | Always | Dialog (A) | BERATUNG | Unlocke |
| HKLINDTWORTH | Holger | Klindtworth | Always | Always | Dialog (A) | BERATUNG | Unlocke |
| IBS01 | | Schulungsteilnehmer | Always | 2010-03-09 | Dialog (A) | SCHULUNG | Unlocke |
| IBS02 | | Schulungsteilnehmer | Always | 2010-03-08 | Dialog (A) | SCHULUNG | Unlocke |
| IBS03 | | Schulungsteilnehmer | Always | 2009-09-09 | Dialog (A) | SCHULUNG | Unlocke |
| IBS04 | | Schulungsteilnehmer | Always | Always | Dialog (A) | SCHULUNG | Unlocke |
| IBS05 | | Schulungsteilnehmer | Always | Always | Dialog (A) | SCHULUNG | Unlocke |
| IBS06 | | Schulungsteilnehmer | Always | Always | Dialog (A) | SCHULUNG | Unlocke |
| IBS07 | | Schulungsteilnehmer | Always | Always | Dialog (A) | SCHULUNG | Unlocke |

**Figure 150 - single profile details window (users)**

Tab page: *Authorizations*

The *Authorizations* tab page shows information on the authorizations contained in the profile, including any authorization objects or fields and field values. Expand an authorization contained in the profile to see where the authorization gets its authorization field values from. Click on the object with blue text to navigate to the corresponding details window.

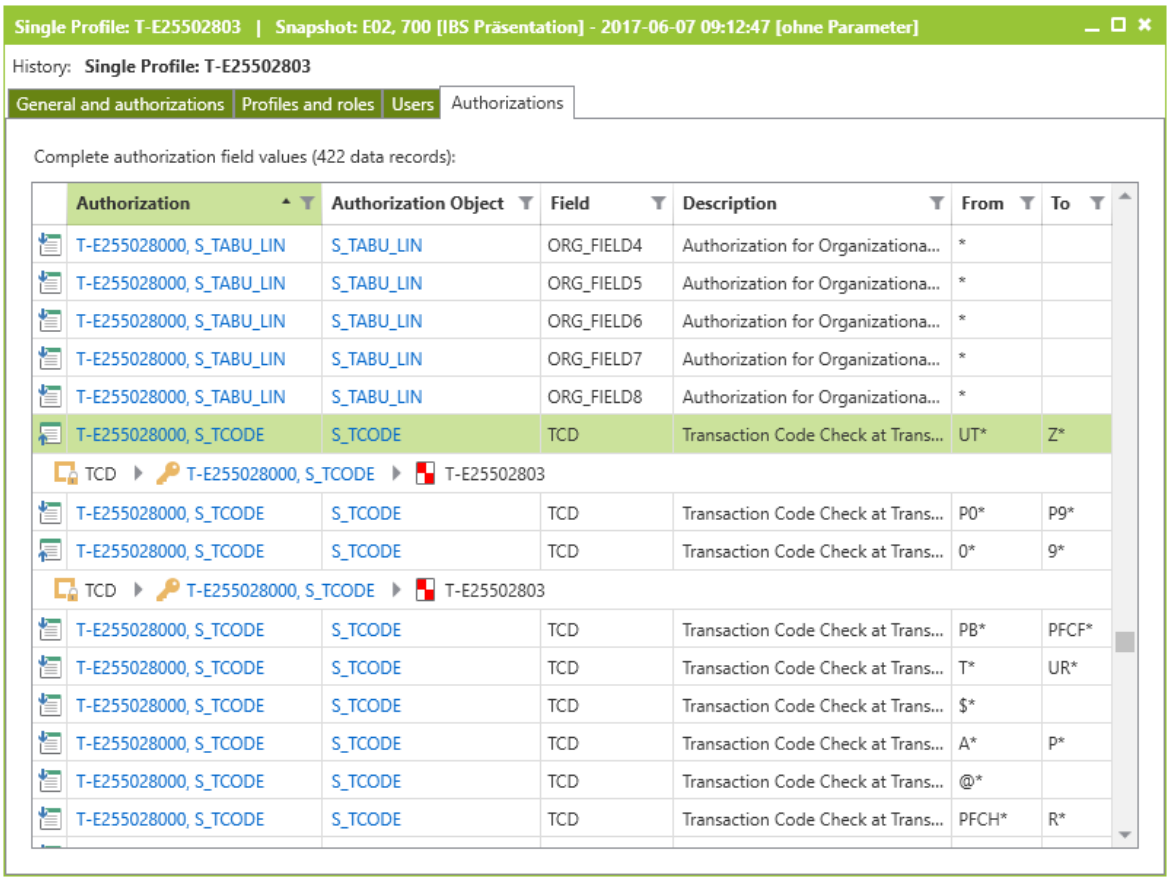



**Figure 151 - singlel profile details window (authorizations)**

### III - 4.1.8 Details window - Composite profile

Tab page: *General*

The *General* tab page contains information about the composite role and the single profiles contained in the composite profile as well as descriptions of them. Click on the object with blue text to navigate to the corresponding details window.

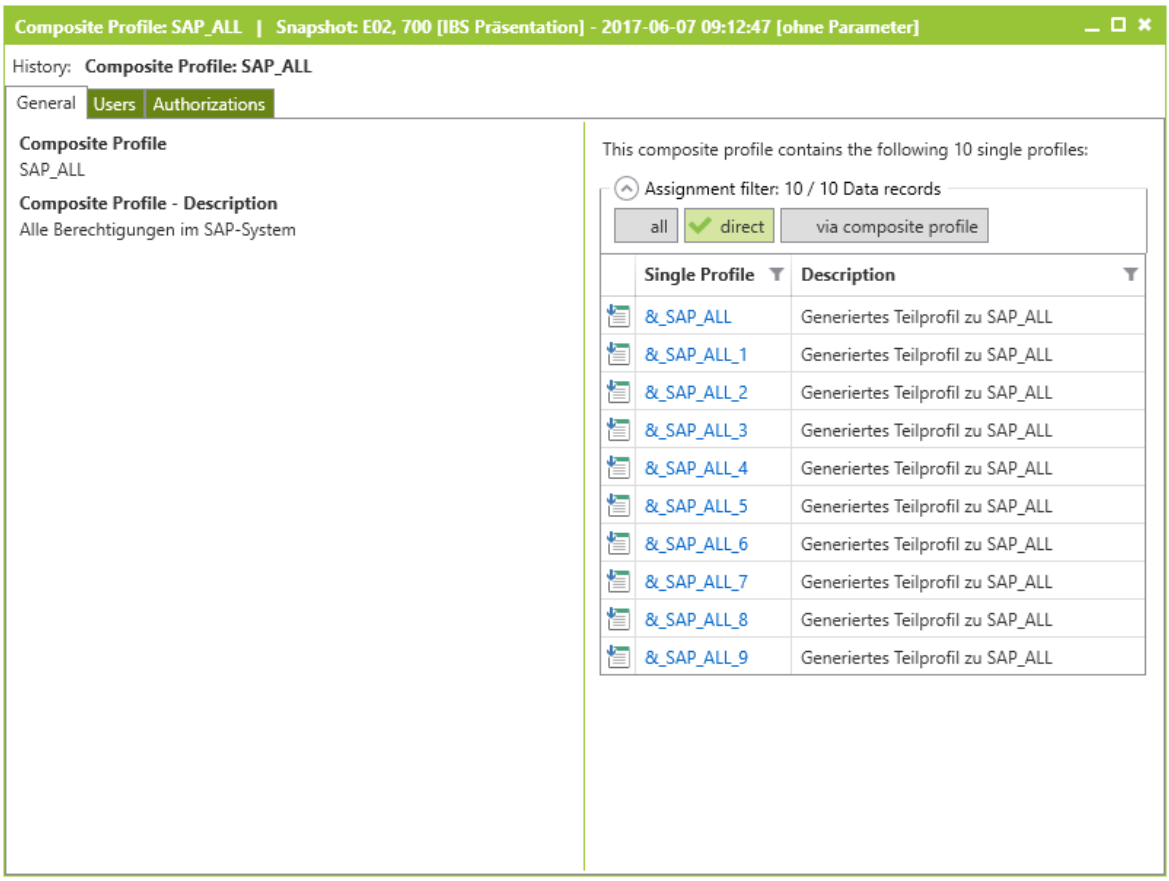



**Figure 152 - Composite profile details window (general)**

*Users and Authorizations* tab pages: the same as the description in the chapter *Details Window – Individual Profile*

### III - 4.1.9 Details window - Single and composite roles

Tab page: *General*

The *General* tab page contains information about the single role, such as a description, who created it, etc. The right-hand side of the details window shows which composite roles or profiles contain the single role. Click on the object with blue text to navigate to the corresponding details window.

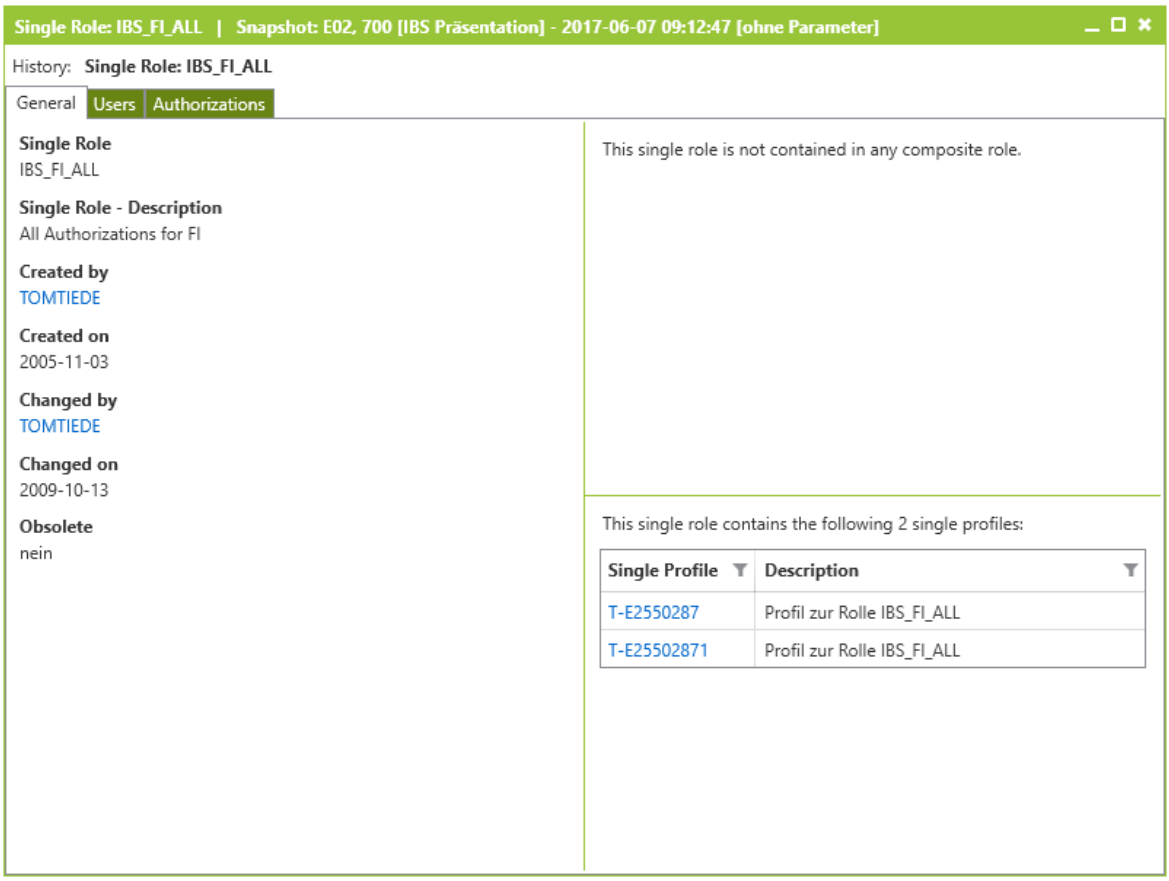



**Figure 153 - Composite profile details window (general)**

*Users and Authorizations* tab pages: the same as the description in the chapter *Details Window – Single Profile*

### III - 4.1.1(Details window - Users

Tab page: *General*

The *General* tab page contains extensive information on the selected user, including name, validity, user type, etc.

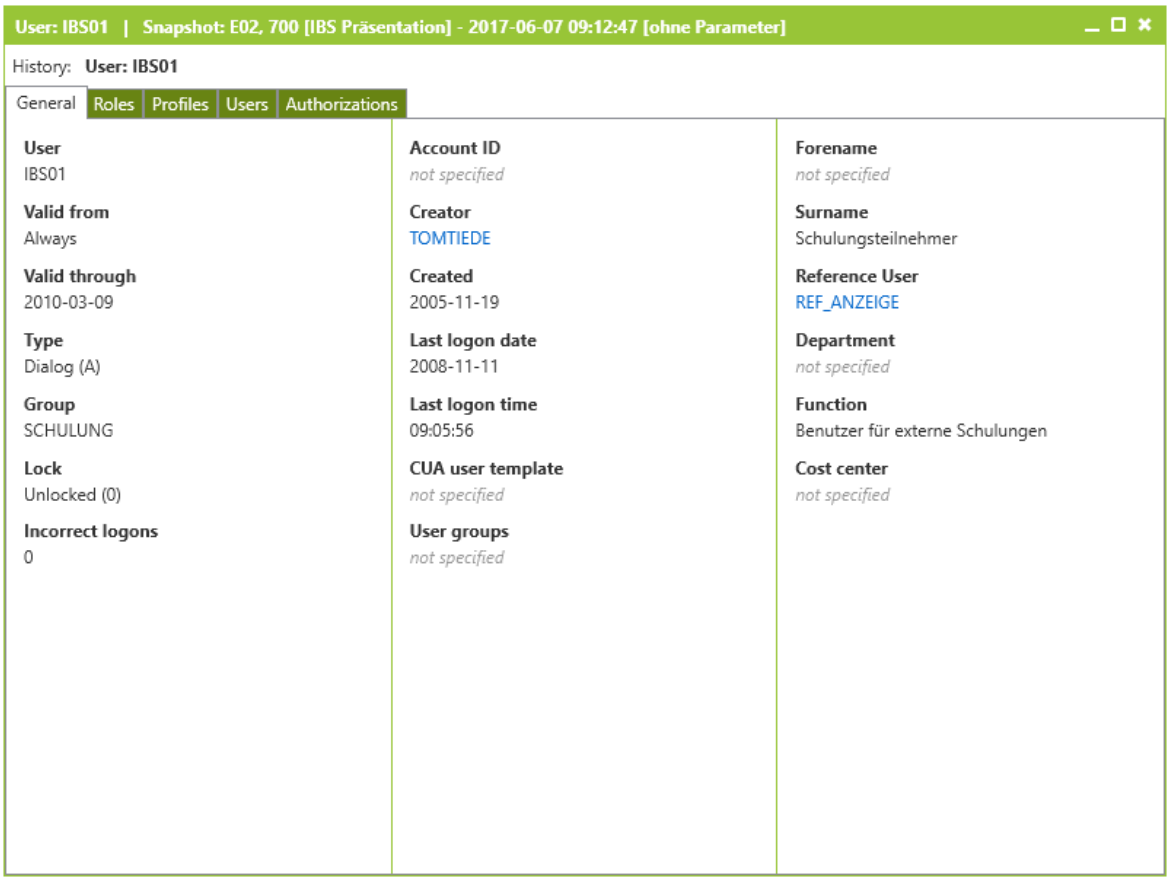



**Figure 154 - User details window (general)**

Tab page: *Roles*

The Roles tab page shows which single or composite roles are assigned to the user. The assignment filter allows filtering of the assigned roles by the following criteria: All , Direct, via reference user, via composite role. Expand  the corresponding role to see whether an single role comes from a composite role or whether reference users exist. Click on the object with blue text to navigate to the corresponding details window..

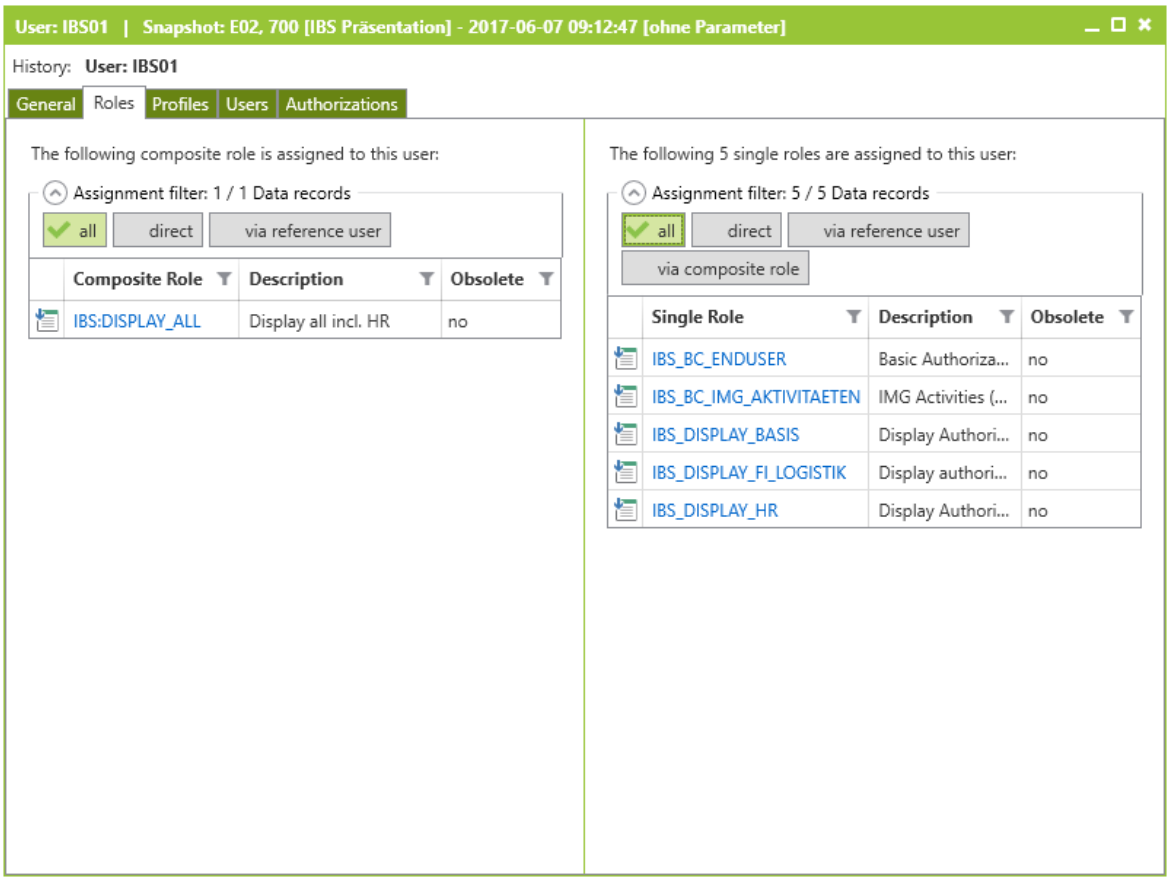



**Figure 155 - User details window (roles)**

Tab page: Profiles

The Profiles tab page shows which individual or composite profiles are assigned to the user. The assignment filter allows filtering of the assigned profiles by the following criteria: All, Direct, via reference users, via composite role, via single role, via composite profile. Expand the corresponding profile to see, for example, whether an individual profile comes from a composite profile. Click on the object with blue text to navigate to the corresponding details window.

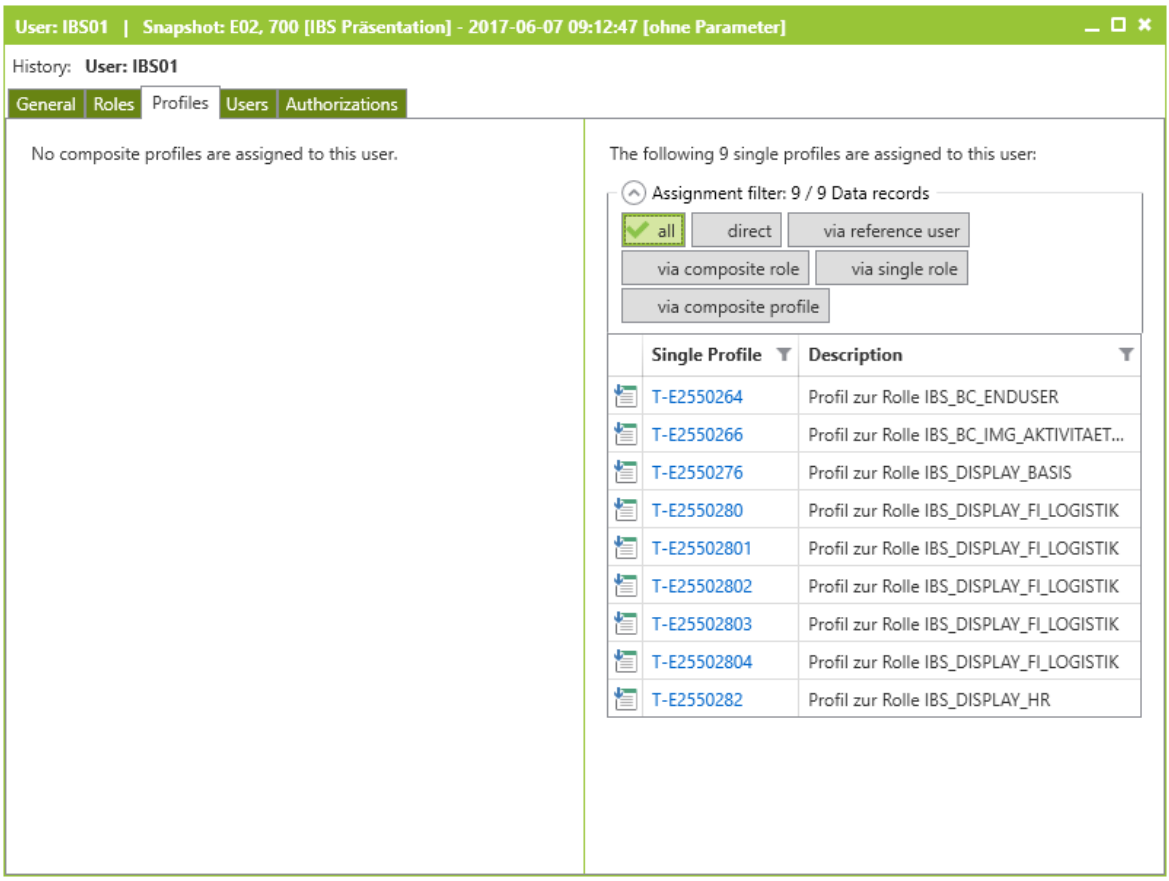



**Figure 156 - User details window (profiles)**

*Users and Authorizations* tab pages: the same as the description in the chapter *Details Window – Individual Profile.*

## III - 4.2 Results display for an authorization query (HANA DB)

### III - 4.2.1 Authorized users tab

The following results window shows the standard table view for an authorization query for authorized HANA DB users:

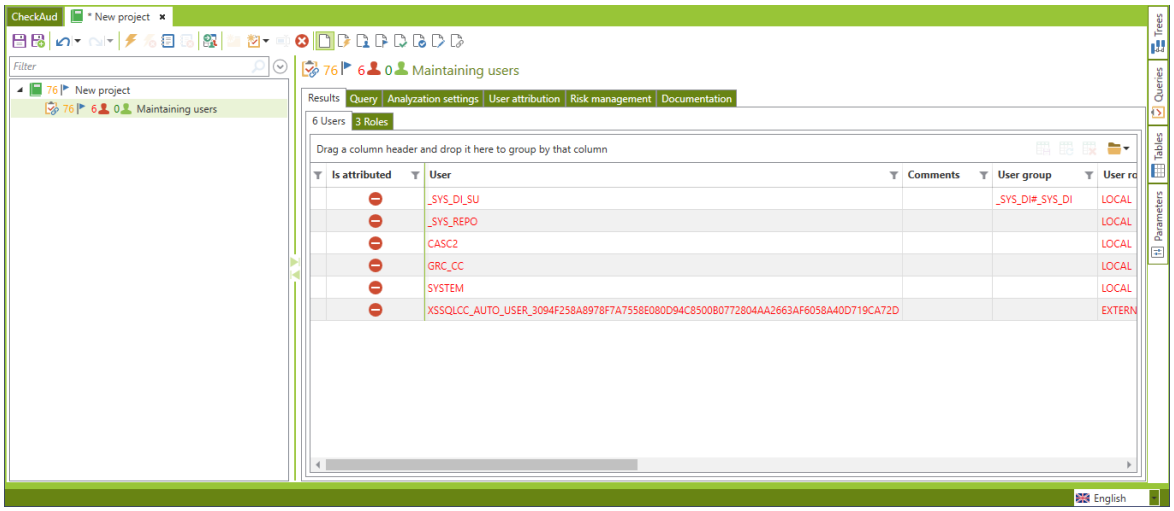



**Figure 157 - Authorization query table view: Authorized users**

In the table, you can display additional information for the columns by moving the mouse over the different fields.

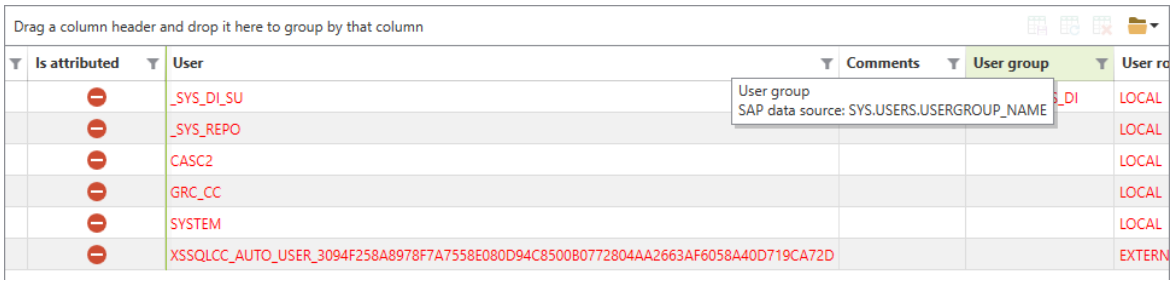



**Figure 158 - Detailed information about the columns**

By default, the query result is displayed only as a table. To display the origin of the authorization objects contained in the query for any user in the table, click the table line for the user in question to open a details window containing the authorization origins in the lower area:


**Figure 159 - Result display including authorization origins for a selected user**

By default, the origins of the authorizations are displayed by privilege type:

- Application privileges
- System privileges
- Package privileges
- Analytic privileges
- Object privileges

Expand the tree to see the full list of that user's authorizations and their origins:

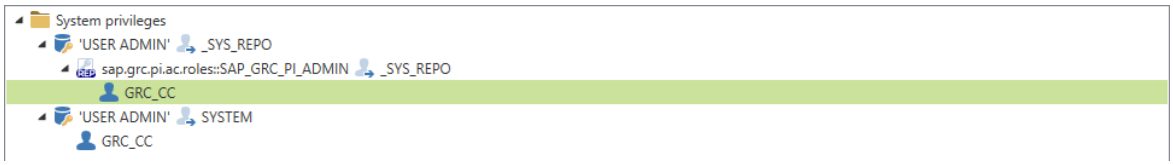



**Figure 160 - Origin and value of an authorization object**

he following symbols are used to represent authorization origins:

| | |
|---|---|
|  | System privilege |
|  | Object privilege |
|  | Package privilege |
|  | Application privilege |
|  | Analytic privilege |
|  | Role (generic) |

| | |
|---|---|
| | Repository role |
| | Catalog role |
| | Hana Deployment Infrastructure role |
| | Grantor |
| | Object owner |
| | Grantable |

As an alternative to the standard display of authorization origins subdivided into application and transaction authorizations, the  button can be used to switch to the view of the participating roles:


**Figure 161 - Authorization origin of a user from the view of the participating roles**

The results are displayed in short form in the analysis project:


**1 2 3 4 5**

1 - Symbol for calculated query incl. color-coding according to score
2 - Calculated score (0 = low system security and 100 = high system security)
3 - Number of technically authorized users (not legitimized according to target specification)
4 - Number of technically authorized users (legitimized according to target specification)
5 - Name of the query

### III - 4.2.2 Authorized users tab compairing snapshots

The results of a HANA DB query using a snapshot comparison is similar to the procedure described in chapter Authorized users tab compairing snapshots 97

### III - 4.2.3 Authorized roles tab

Use the *Roles* tab to create a table displaying the roles that fully include the queried authorization, regardless of whether the role is assigned to any users:

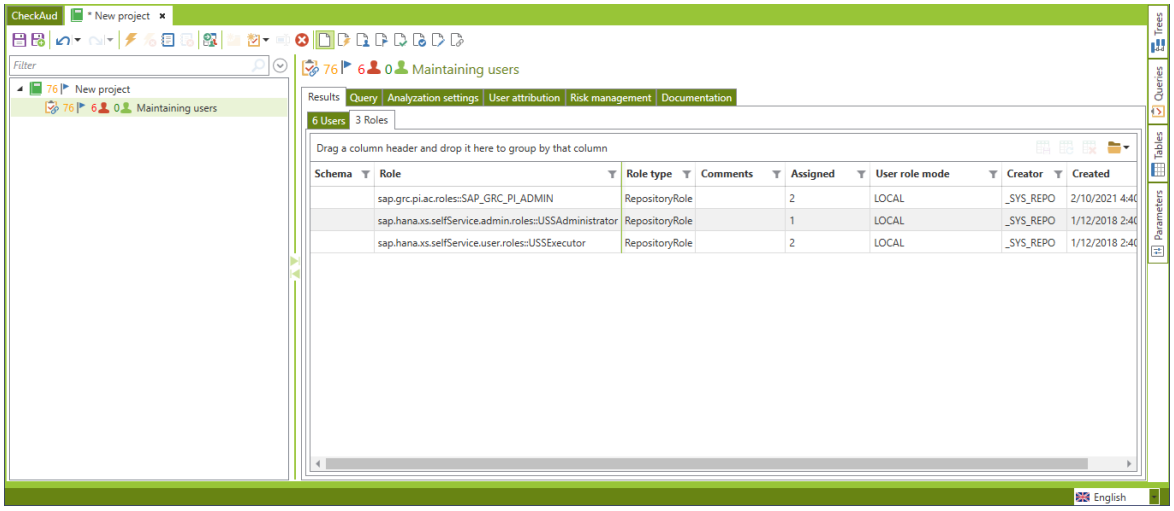



**Figure 162 - Authorization query table view: Authorized roles**

When you select a role, you can display the origins of the authorizations for this selected role.

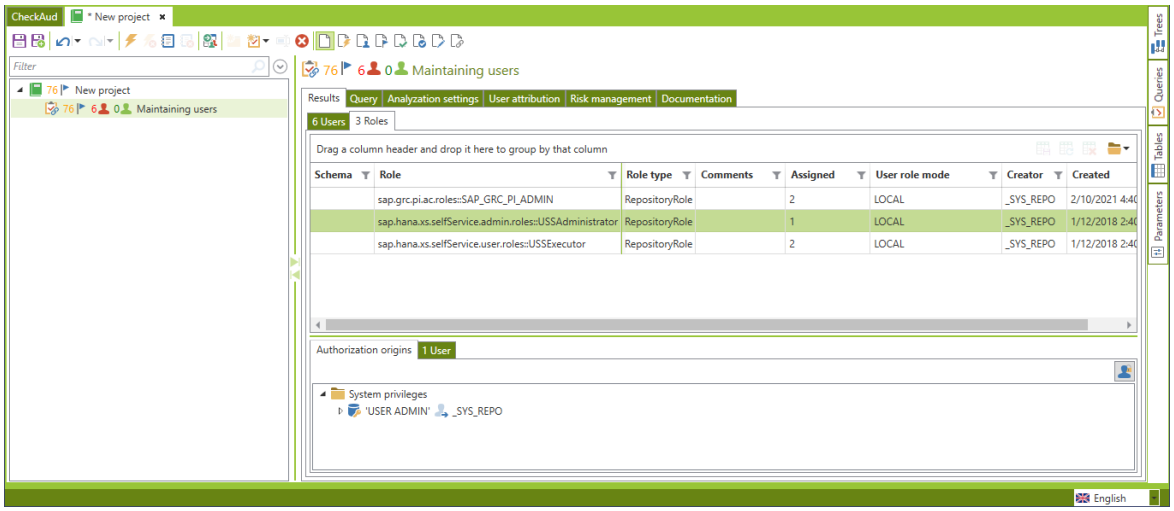



**Figure 163 - Origins of the authorizations of a composite role**

By default, the origins of authorizations are displayed by authorization type.


**Figure 164 - List of authorizations in a role**

Select the *Users* tab to list all the users defined in the composite role.

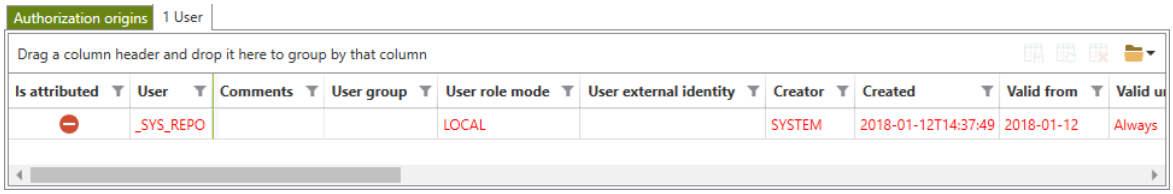



**Figure 165 - Users assigned to the composite role**

You can display the role assignment path of the individual users by selecting the user in question.

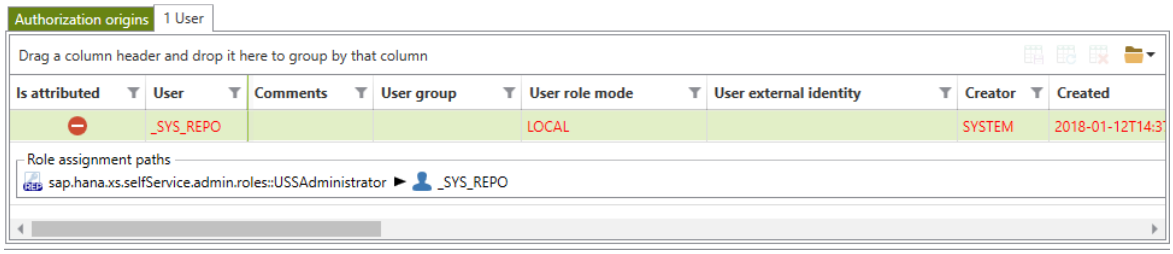



**Figure 166 - Role assignment path of the user**

## III - 4.3 Results display for a table query

The results display for a table query is also a table:

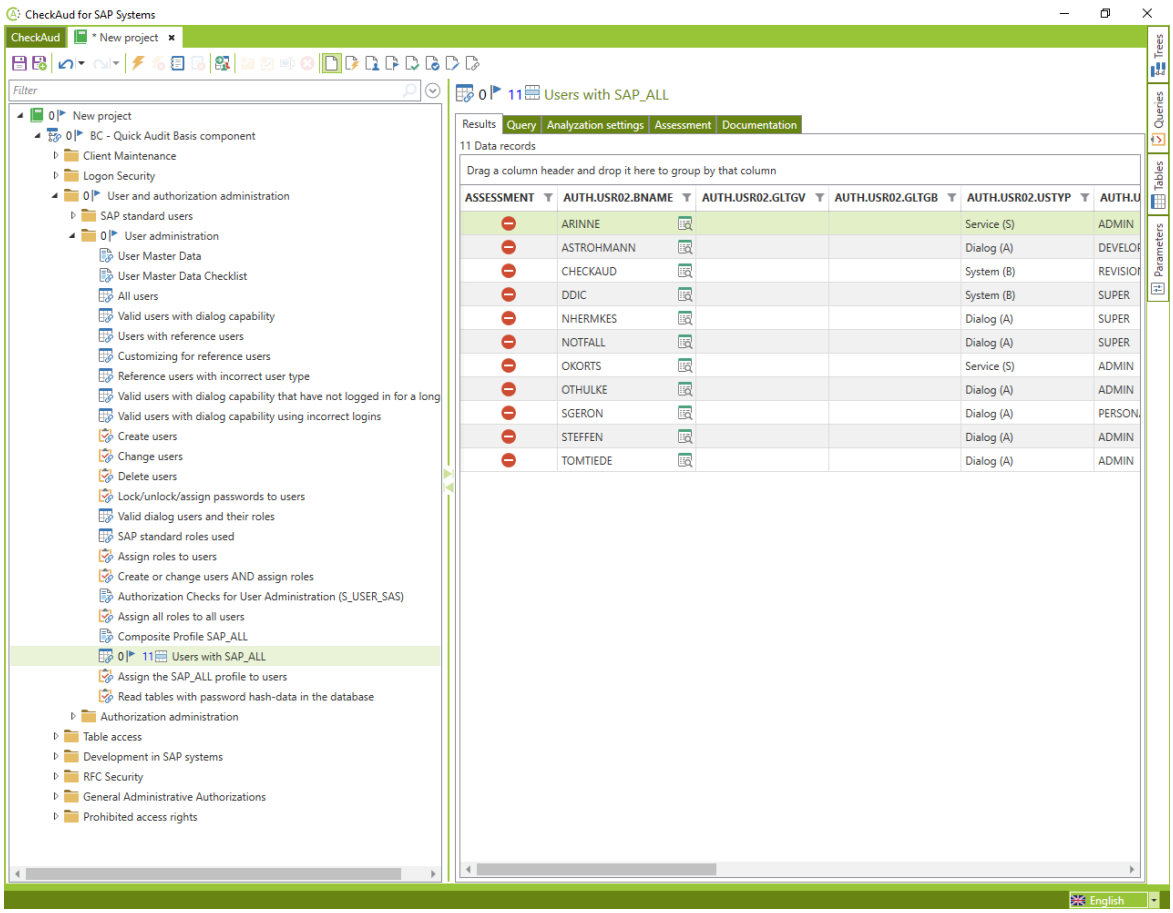



**Figure 167 - Results display for a table query(ABAP table)**

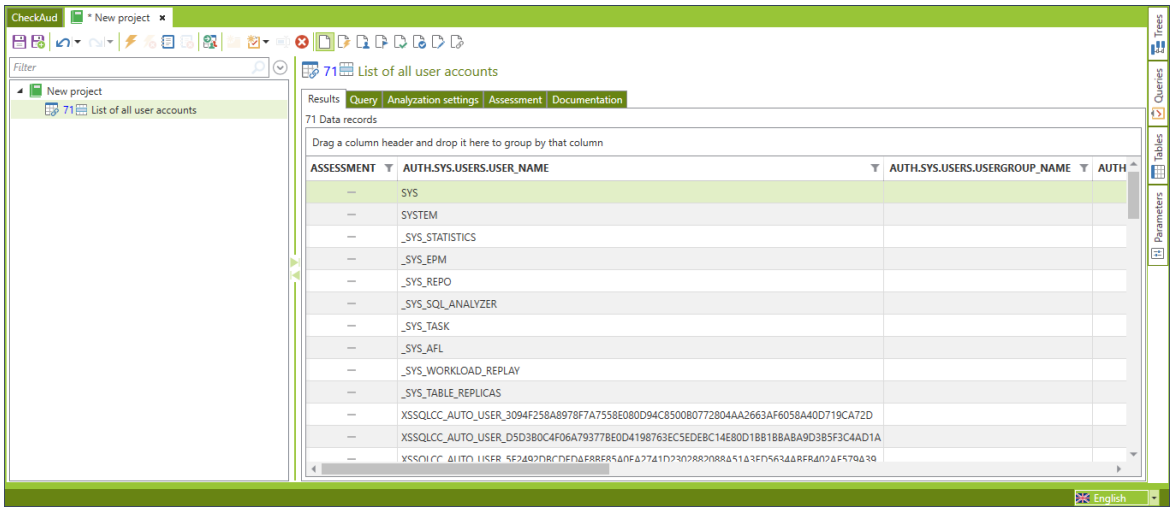



**Figure 168 - Results display for a table query(ABAP table)**

In the table, you can display additional information for the columns by moving the mouse over the different fields.

The *Assessment* column shows whether the table entry meets the requirements:

| | |
|---|---|
|  | Assessment criterion not fulfilled |
|  | Assessment criterion fulfilled |

The table entries can be assessed on the Assessment (Bewertung) tab page. For more detailed information, see the chapter Custom Table Queries.

You can use the  button to display additional information about the selected table entry (only available for ABAP tables).

## III - 4.4 Evaluating user statistics

In order to evaluate user statistics in CheckAud, the data must first be extracted with the help of CheckScan (see Chapter II 5.5 and 5.6 ). It is possible to evaluate the user statistics in a personalized or anonymized way. For this purpose, four tables are available in the table sets IBS_STATISTICS (anonymized) and IBS_USER_STATISTICS (personalized).

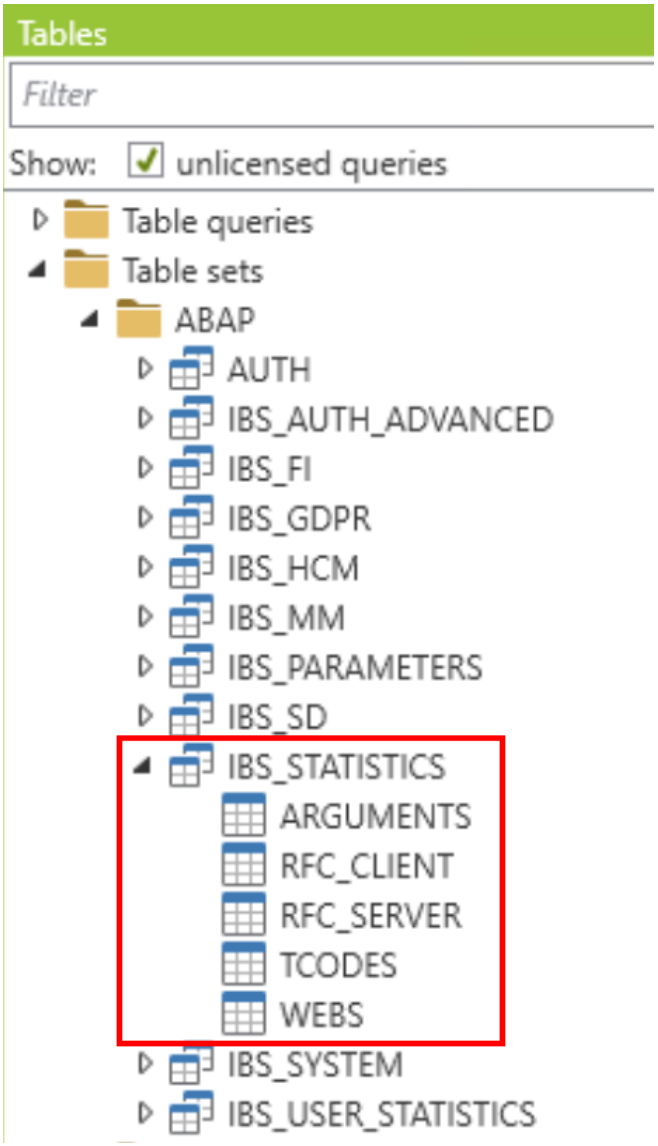



**Figure 169 - Tables anonymized user statistics**

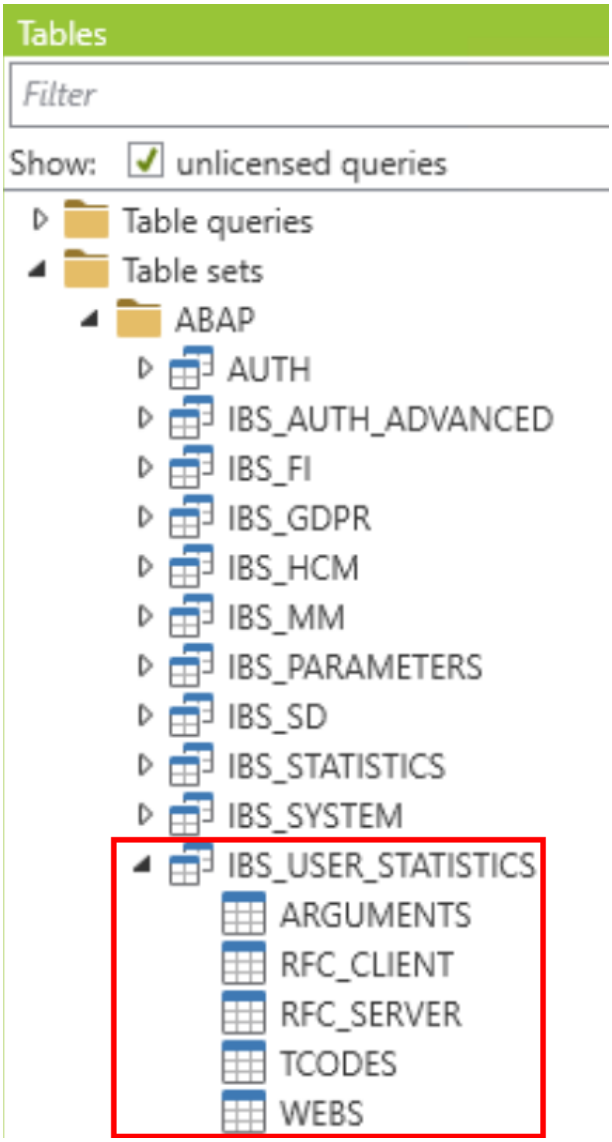



**Figure 170 - Tables personalized user statistics**

**ARGUMENTS table**

In the Arguments table the deducted months (always shown with the first of the month) are output. In the SAP standard, the transaction calls of the last 90 days are logged, which means that there are usually four entries in the table. However, this does not mean that the four months are completely included but only affected.

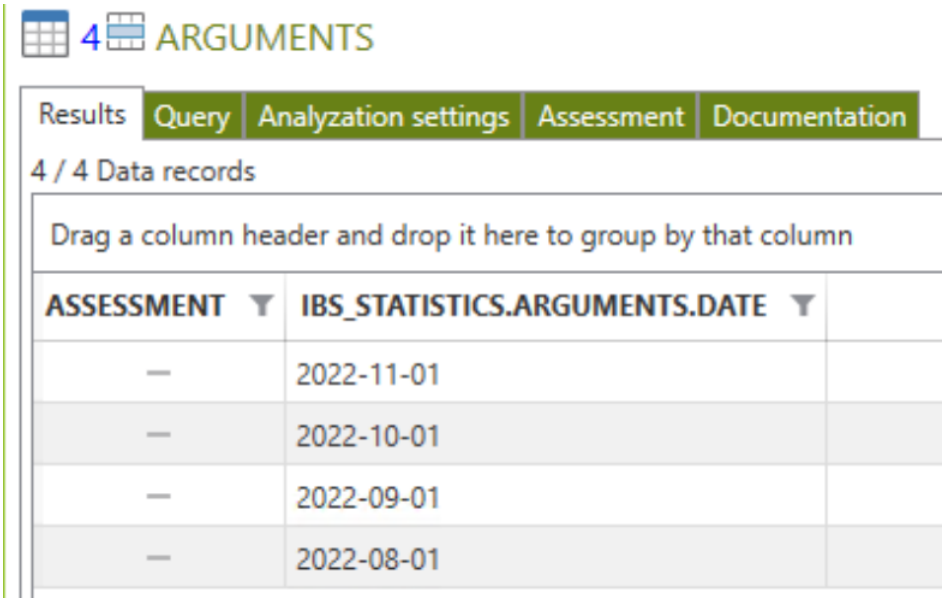



**Figure 171 - ARGUMENTS table**

### Tables RFC_SERVER and RFC_CLIENT

In SAP, for each RFC call, the system logs which user as RFC client or RFC server executed the call. The respective RFC calls are output in the RFC_SERVER and RFC_CLIENT tables. In the personalized usage statistics, the user is also output in the anonymized one not.

### Table TCODES

In the table TCODES the used transaction codes are displayed. In the anonymized statistics the number of users per transaction is displayed and in the personalized statistics the user per transaction code is displayed. The Entry-Job column shows whether the call was made via SAP-job.

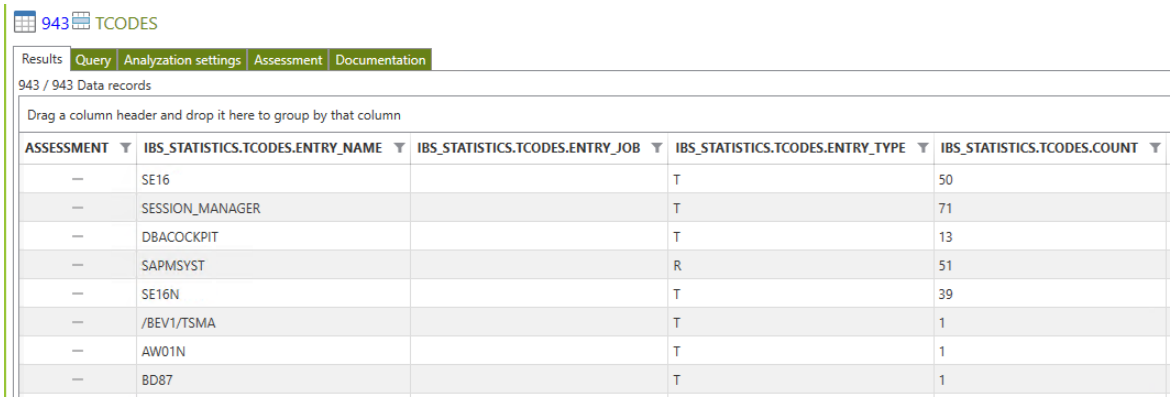



**Figure 172 - Table TCODES anonymized**

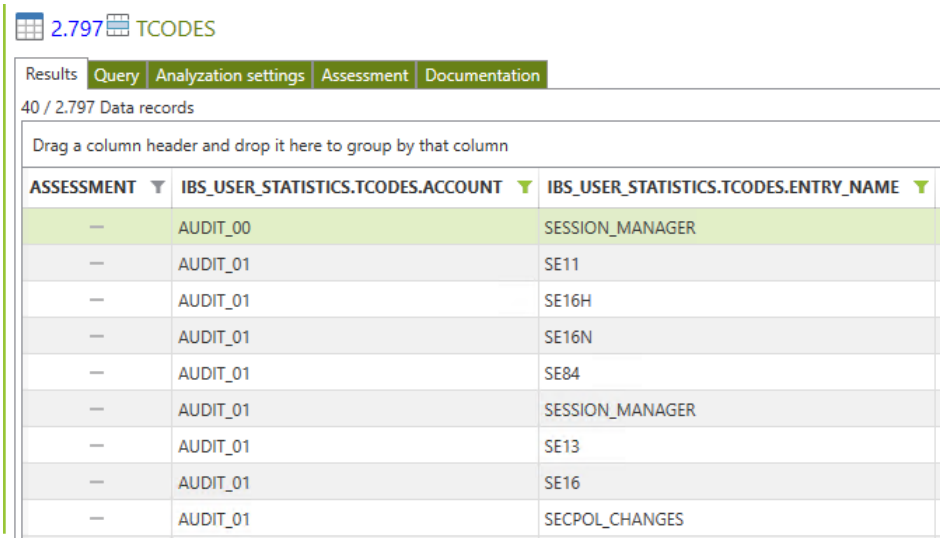



**Figure 173 - Table TCODES personalized**

### Table WEBS

All Fiori app calls are displayed in the WEBS table.

## III - 4.5 Results display for a parameter query

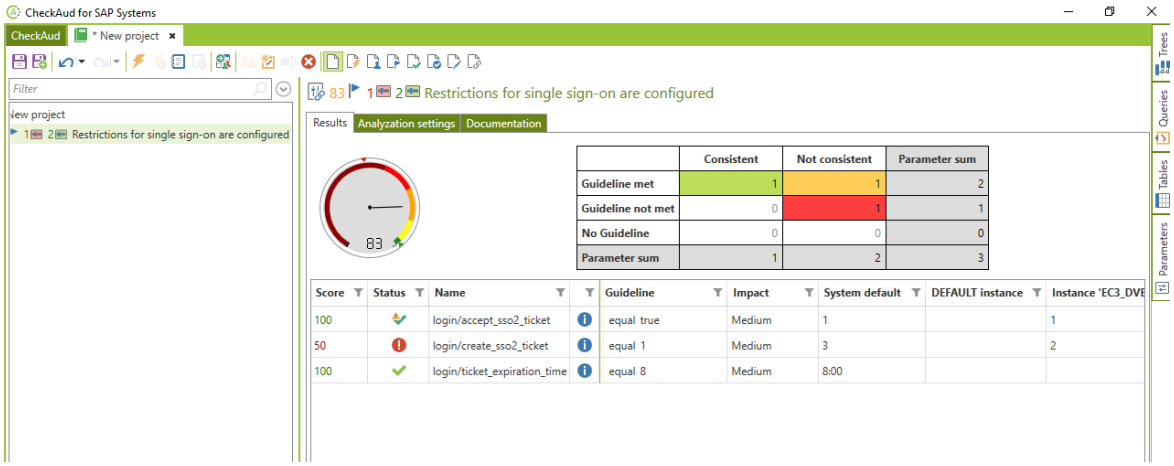



**Figure 174 - Results display for a parameter evaluation**

Fulfilled requirements are flagged with the ✔ symbol after the analysis is performed. If the default values defined in CheckAud differ from the parameter values set in the SAP system, they are flagged with a ❗ symbol.

| | Consistent | Not consistent | Parameter sum |
|---|---|---|---|
| Guideline met | 1 | 1 | 2 |
| Guideline not met | 0 | 1 | 1 |
| No Guideline | 0 | 0 | 0 |
| Parameter sum | 1 | 2 | 3 |

**Figure 175 - Summary**

The parameters defined in the parameter queries are summarized in a matrix:

| | |
|---|---|
| *Requirement is fulfilled and consistent* | The requirement is fulfilled and the parameter is consistent on all SAP system instances |
| *Requirement is fulfilled and inconsistent* | The requirement is fulfilled and the parameter is not consistent on all SAP system instances |
| *Requirement is not fulfilled and is consistent* | The requirement is not fulfilled and the parameter is consistent on all SAP system instances |
| *Requirement is not fulfilled and is inconsistent* | The requirement is not fulfilled and the parameter is not consistent on all SAP system instances |
| *No requirement and consistent* | No requirement is maintained and the parameter is consistent on all SAP system instances |
| *No requirement and inconsistent* | No requirement is maintained and the parameter is not consistent on all SAP system instances |

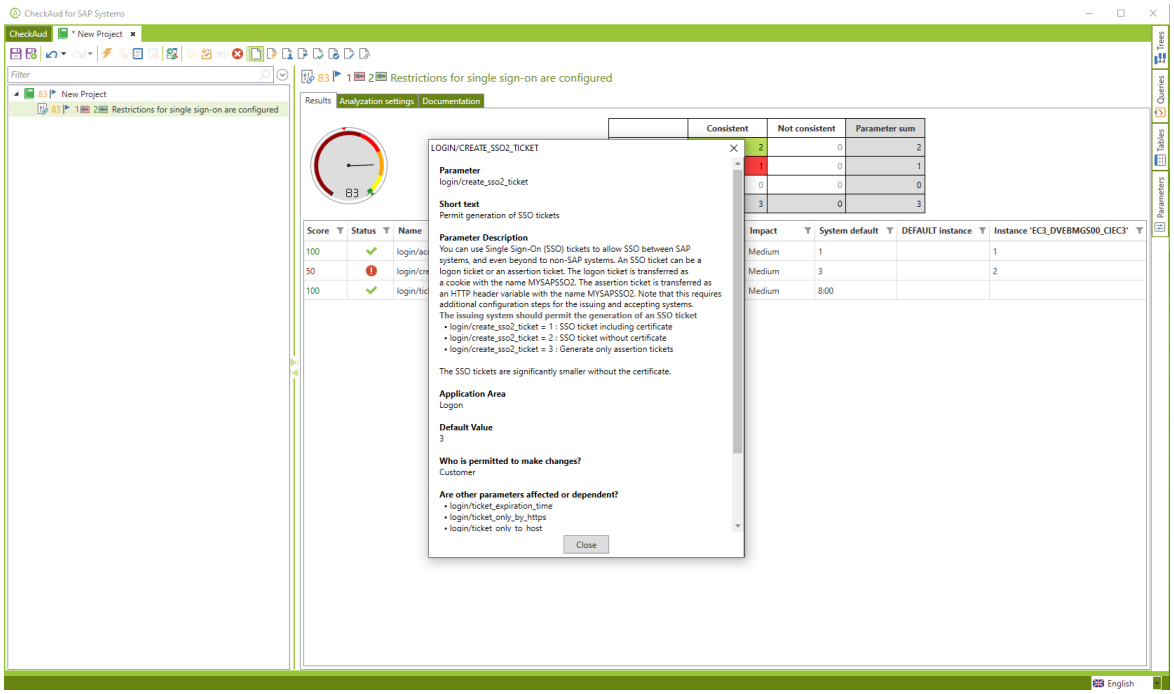



**Figure 176 - SAP documentation for a parameter**

The icon opens the SAP documentation for the selected parameter. The detailed information included in the documentation was read out and transferred from the SAP system.

**Note:** parameter queries are only available for ABAP systems.

## III - 4.6 Custom layouts for the table display

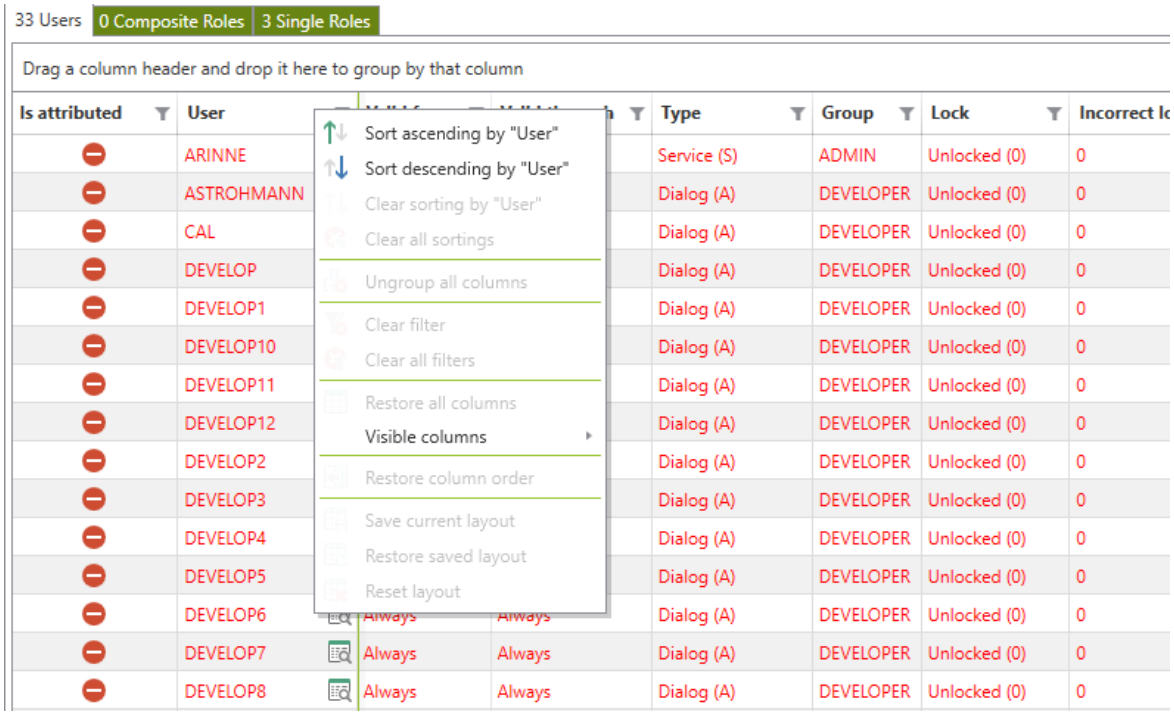
The layouts of the table views for the various result displays for authorization queries, table queries and parameter queries can be customized.

### III - 4.6.1 Sorting in a table view

Results can be sorted by column by clicking the desired column header. Each time that you click, the option changes between:

No sorting --> Sorting in ascending order --> Sorting in descending order --> No sorting


You can only ever sort by one column in the table. Alternative, you can use the context menu to configure the sorting (by right-clicking the column in question):

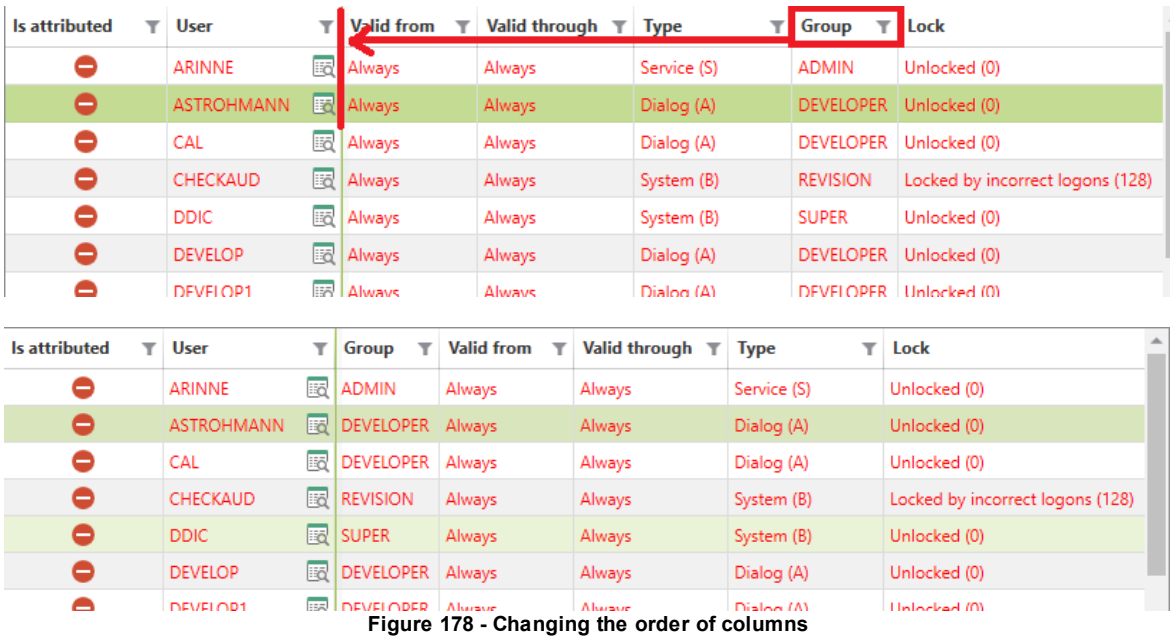



| Is attributed | User | Valid from | Valid through | Type | Group | Lock | Incorrect lc |
|---|---|---|---|---|---|---|---|
| | ARINNE | | | Service (S) | ADMIN | Unlocked (0) | 0 |
| | ASTROHMANN | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | CAL | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP1 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP10 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP11 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP12 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP2 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP3 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP4 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP5 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP6 | | | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP7 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |
| | DEVELOP8 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) | 0 |

**Figure 177 - Context menu for sorting based on a column**

### III - 4.6.2 Changing the order of the columns

You can drag and drop a column header to change its order in the table columns.



| Is attributed | User | Valid from | Valid through | Type | Group | Lock |
|---|---|---|---|---|---|---|
| | ARINNE | Always | Always | Service (S) | ADMIN | Unlocked (0) |
| | ASTROHMANN | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| | CAL | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| | CHECKAUD | Always | Always | System (B) | REVISION | Locked by incorrect logons (128) |
| | DDIC | Always | Always | System (B) | SUPER | Unlocked (0) |
| | DEVELOP | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |

| Is attributed | User | Group | Valid from | Valid through | Type | Lock |
|---|---|---|---|---|---|---|
| | ARINNE | ADMIN | Always | Always | Service (S) | Unlocked (0) |
| | ASTROHMANN | DEVELOPER | Always | Always | Dialog (A) | Unlocked (0) |
| | CAL | DEVELOPER | Always | Always | Dialog (A) | Unlocked (0) |
| | CHECKAUD | REVISION | Always | Always | System (B) | Locked by incorrect logons (128) |
| | DDIC | SUPER | Always | Always | System (B) | Unlocked (0) |
| | DEVELOP | DEVELOPER | Always | Always | Dialog (A) | Unlocked (0) |

**Figure 178 - Changing the order of columns**

**Note:** You cannot change the order of some of the column headers in the tables.

### III - 4.6.3 Showing and hiding columns

If necessary, you can temporarily hide columns that are not required in the result table. To do so, open the context menu by right-clicking the column header in question:

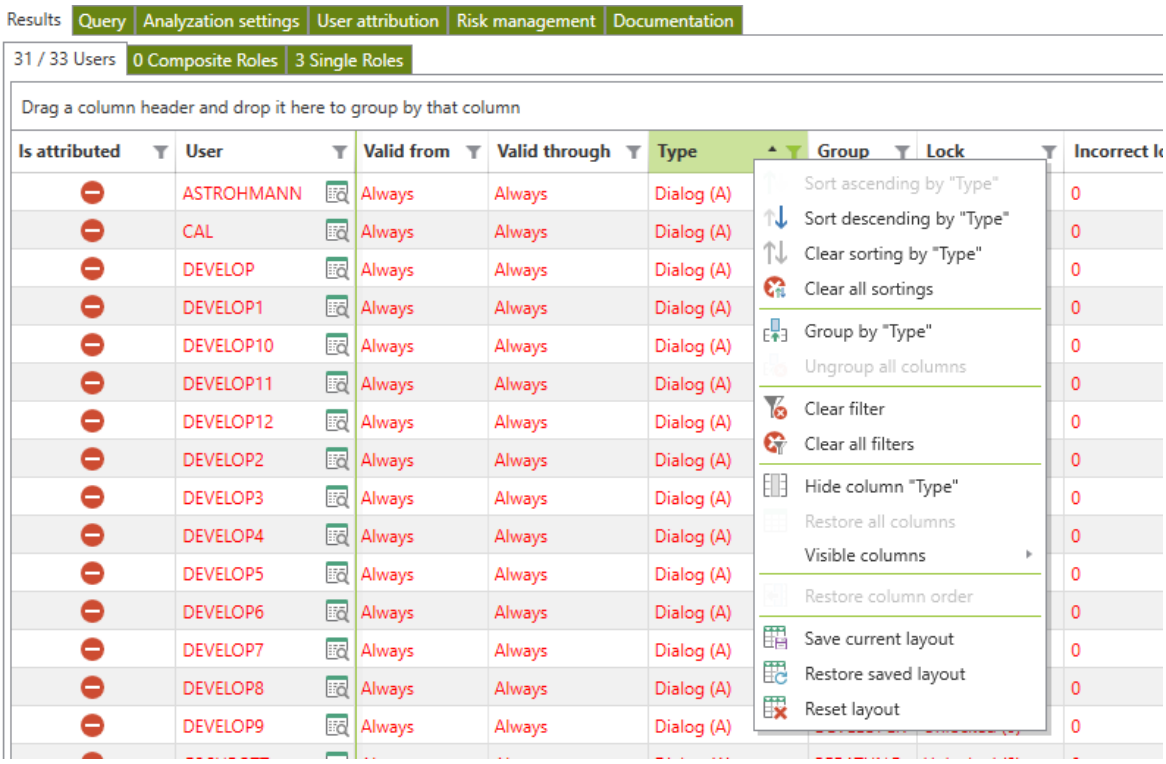



**Figure 179 - Hiding columns that are not required**

To show the columns again, open the context menu and choose *Visible columns*:

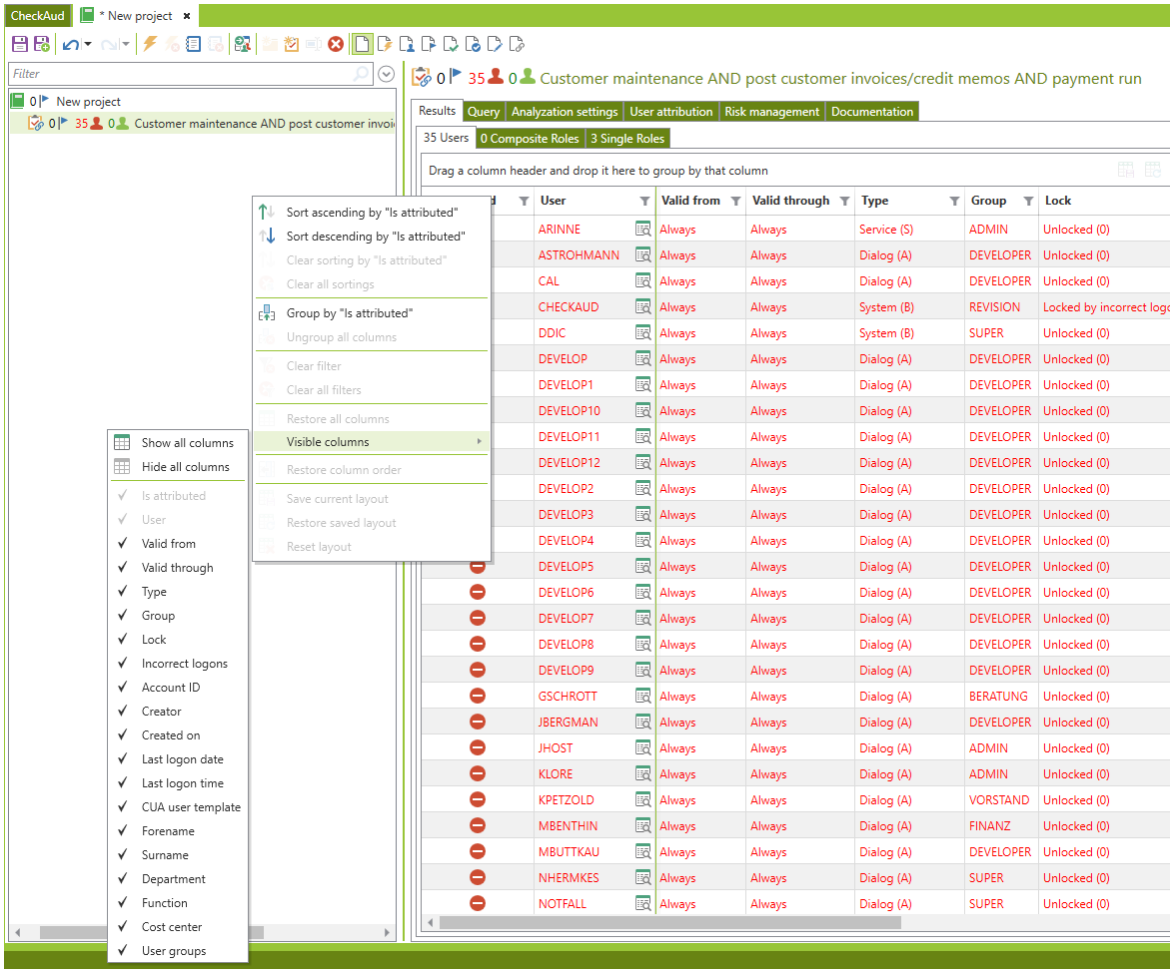



**Figure 180 - Showing hidden columns again**

### III - 4.6.4 Ad-Hoc filter in the table view

Ad hoc filters let you filter the results quickly and can be used in addition to the analysis filters described in the chapter *Analysis Settings*. You can define ad hoc filters using the icon in the respective column headers. The table component provides some standard criteria for creating ad hoc filters.

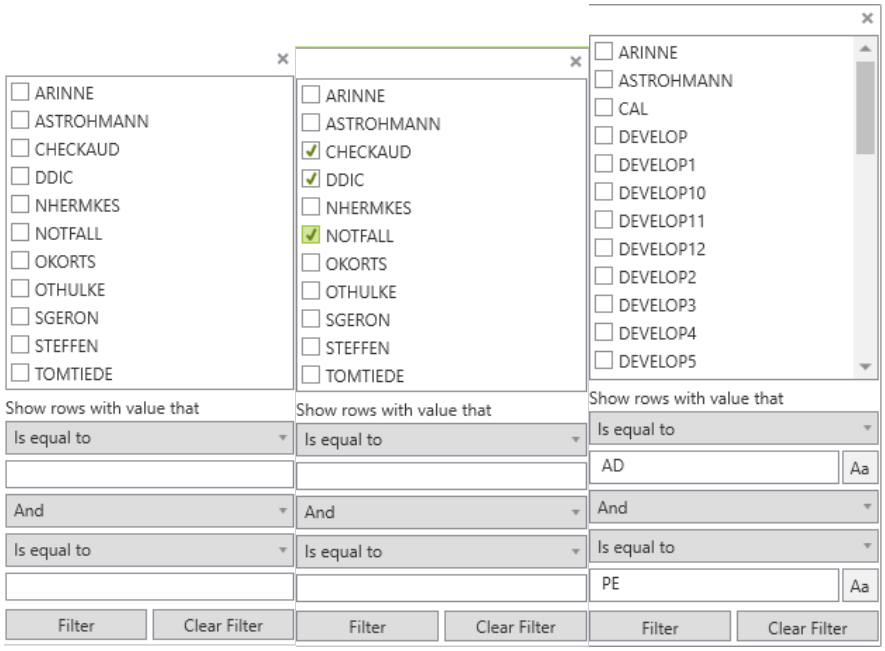



**Figure 181 - Examples of ad hoc filters**

An active ad hoc filter is indicated by the colored icon in each column header.

## III - 4.6.5 Grouping results

You can make groupings in the results display table. To do so, for example, you can drag and drop the desired column header to the row *Drag a column header and drop it here to group by that column* above it::

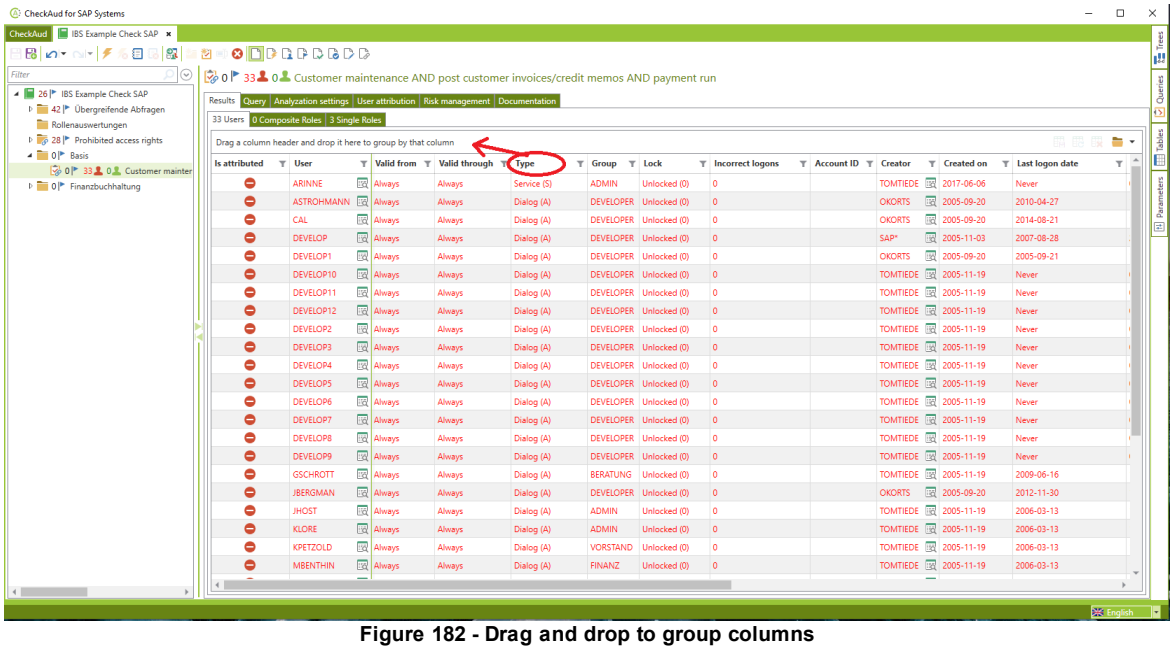



**Figure 182 - Drag and drop to group columns**

Alternatively, you can also right-click the column header to open the context menu and make a grouping based on columns:

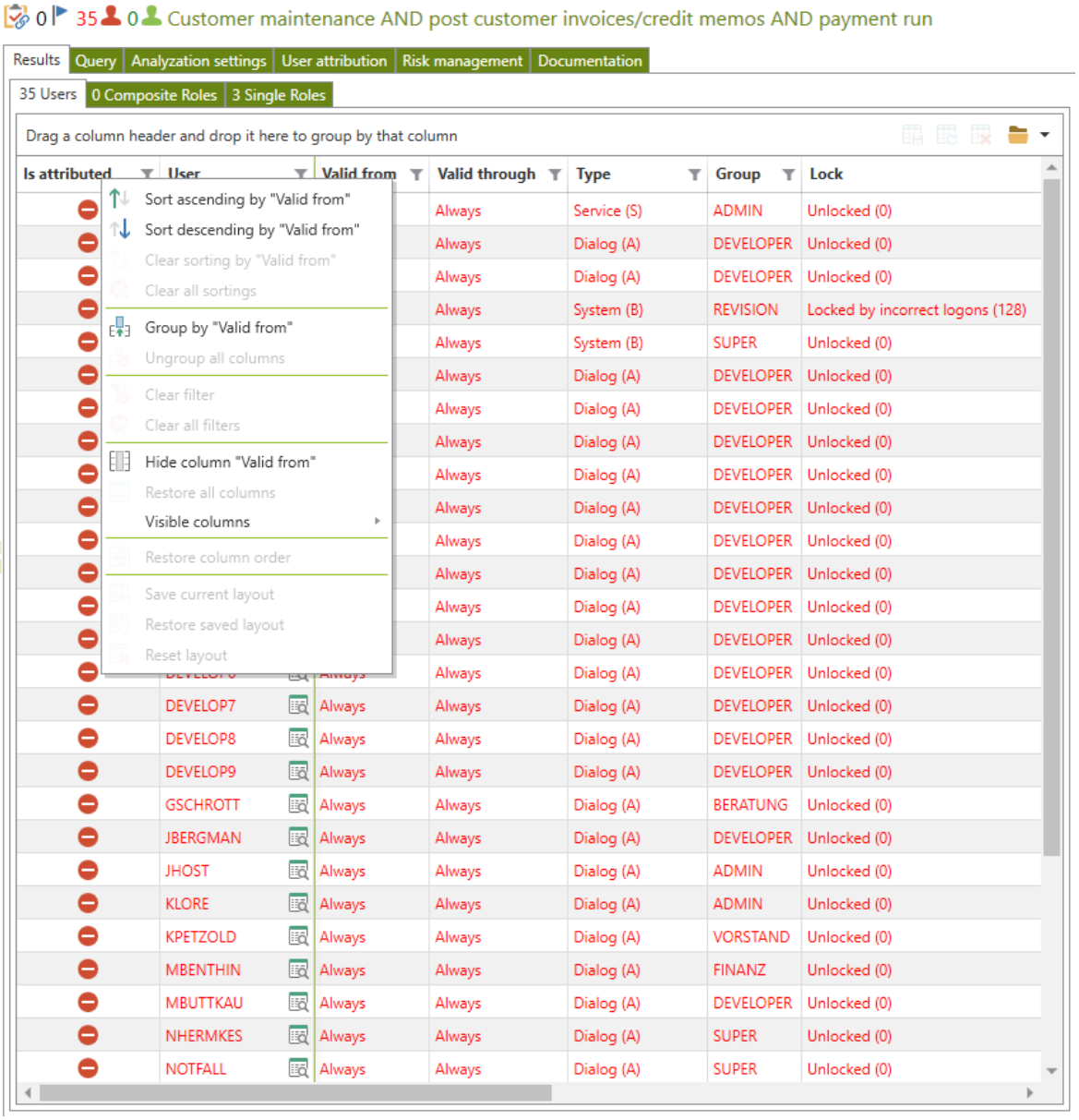



**Figure 183 - Context menu for grouping columns**

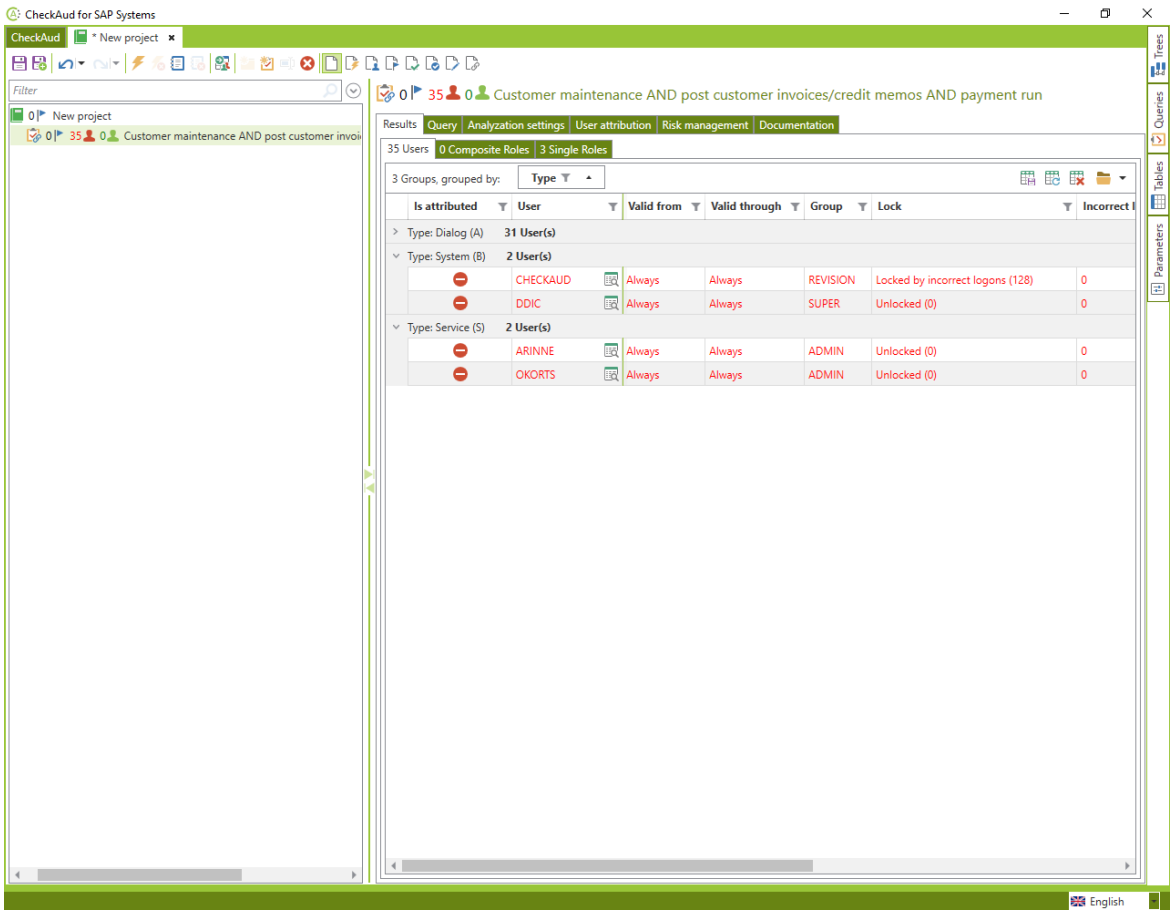



**Figure 184 - Results display with grouping**

To remove the grouping, you can use drag and drop or click the “x” that appears.

### III - 4.6.6 Saving a layout

You can save your created layout as a default layout for other result tables in the analysis project. This layout is then automatically used for each result table.

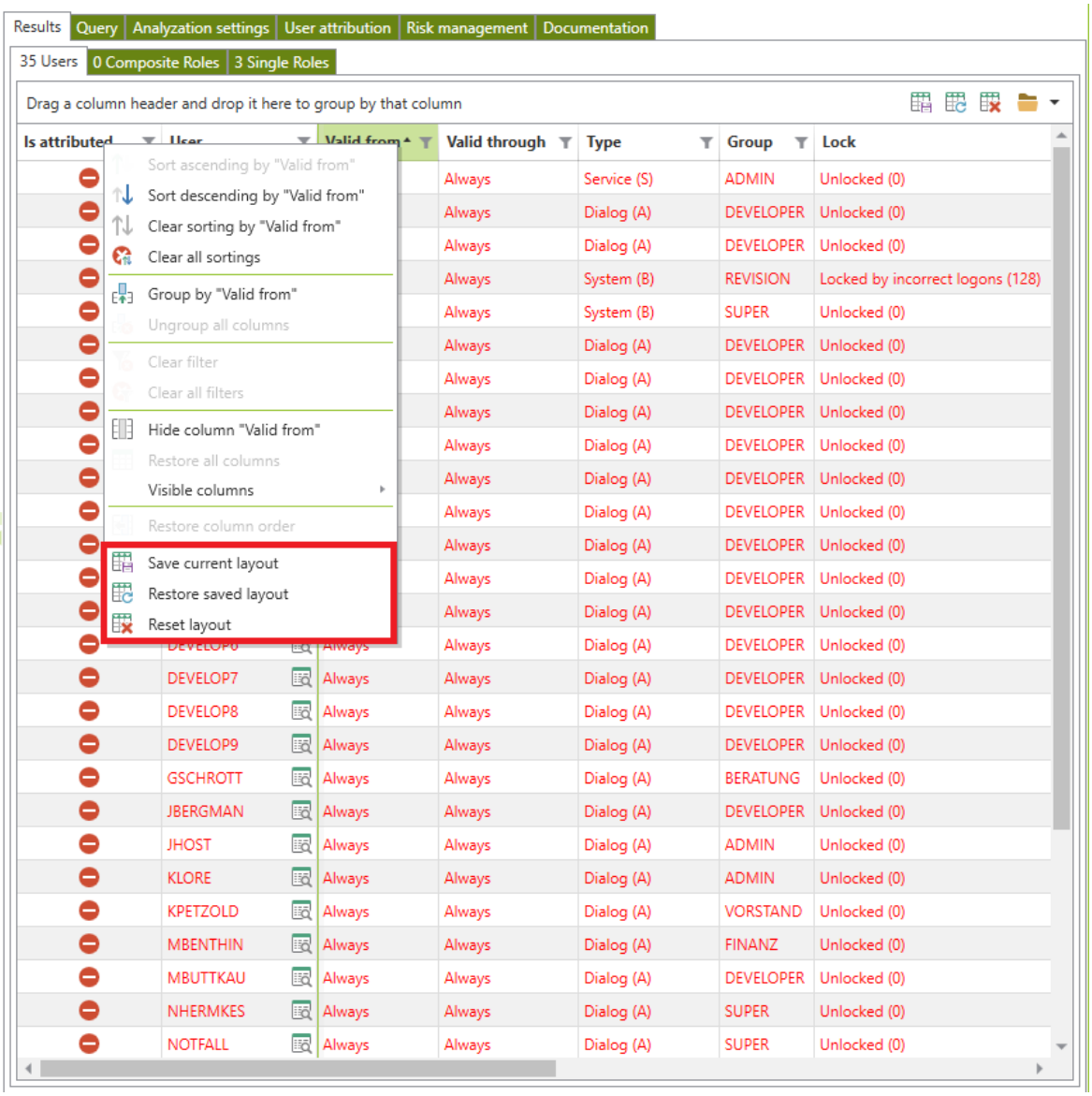



**Figure 185 - Saving the layout**

The context menu includes an option to save the layout. This saves the groupings, adjustments to the column order, shown/hidden columns and the sorting options. It does not save any filter adjustments in the columns. Choose the Reset layout button to return to the initial view. If you have made changes since you last saved the layout, you can choose the Restore saved layout button to revert to the last save point.

The layout can also be saved, reset, or restored in the table header.

After the grouping is configured and saved, the layout can be exported. That allows you to add the layout import and the created grouping to additional projects.

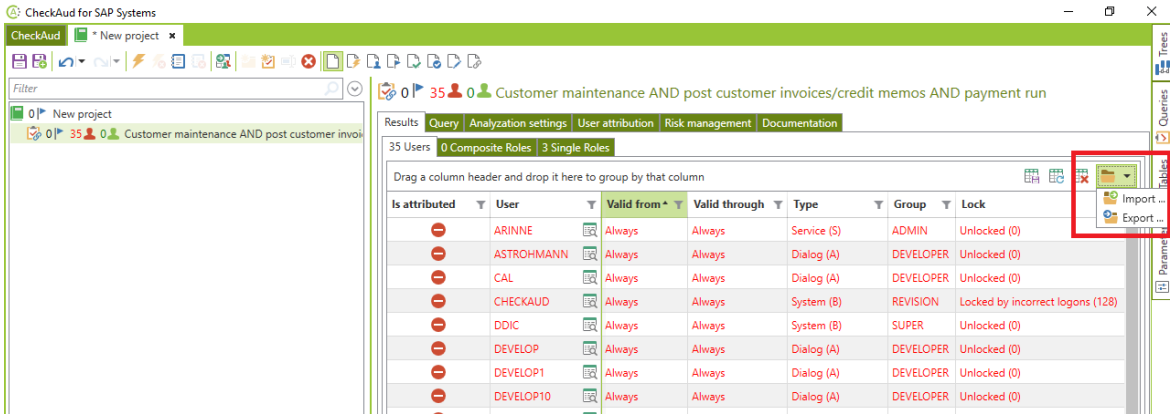



**Figure 186 - Importing/exporting the created layout**

**Note:** The layout of the table view also has an effect on the Excel exports created from the results. They use the same column orders, sorting, and so on, as the ones defined in the table layout in CheckAud.

## III - 5 Exporting the results

You can export the results of an evaluated analysis project for each individual queries, for multiple queries in a subproject or for the whole analysis project. For the partial or full export, an HTML overview is created that provides a link to the individual result files (Excel documents).

## III - 5.1 Exporting an authorization query

An authorization query must be evaluated and selected for the result export. You use the button to start the export. A dialog box for selecting the storage path appears:

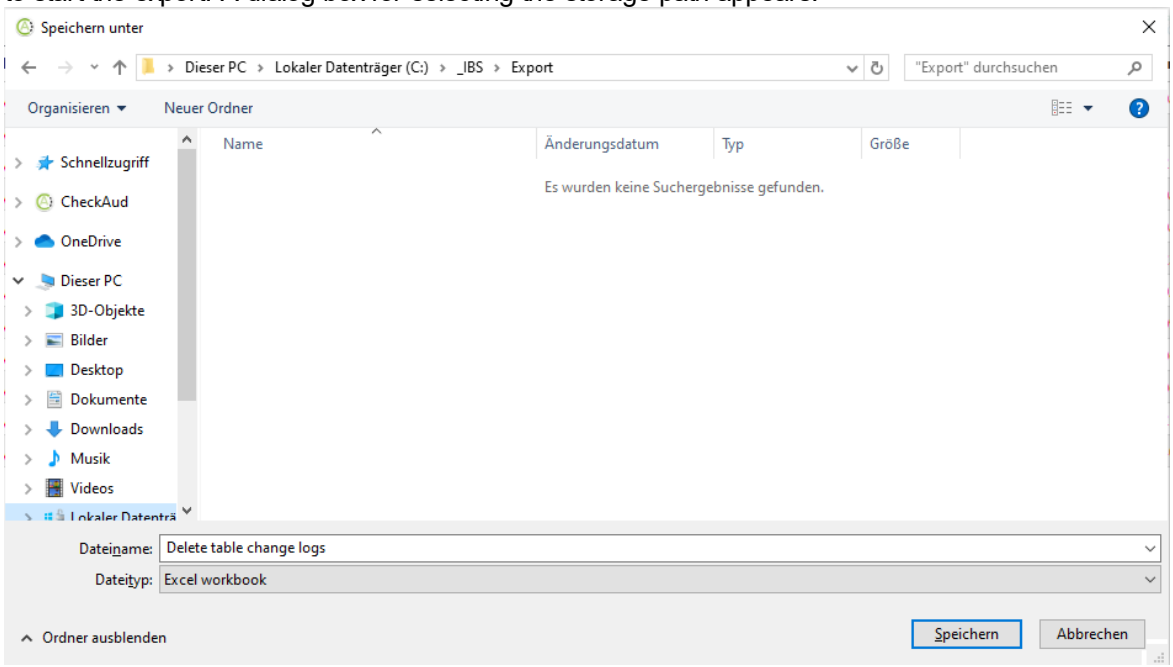
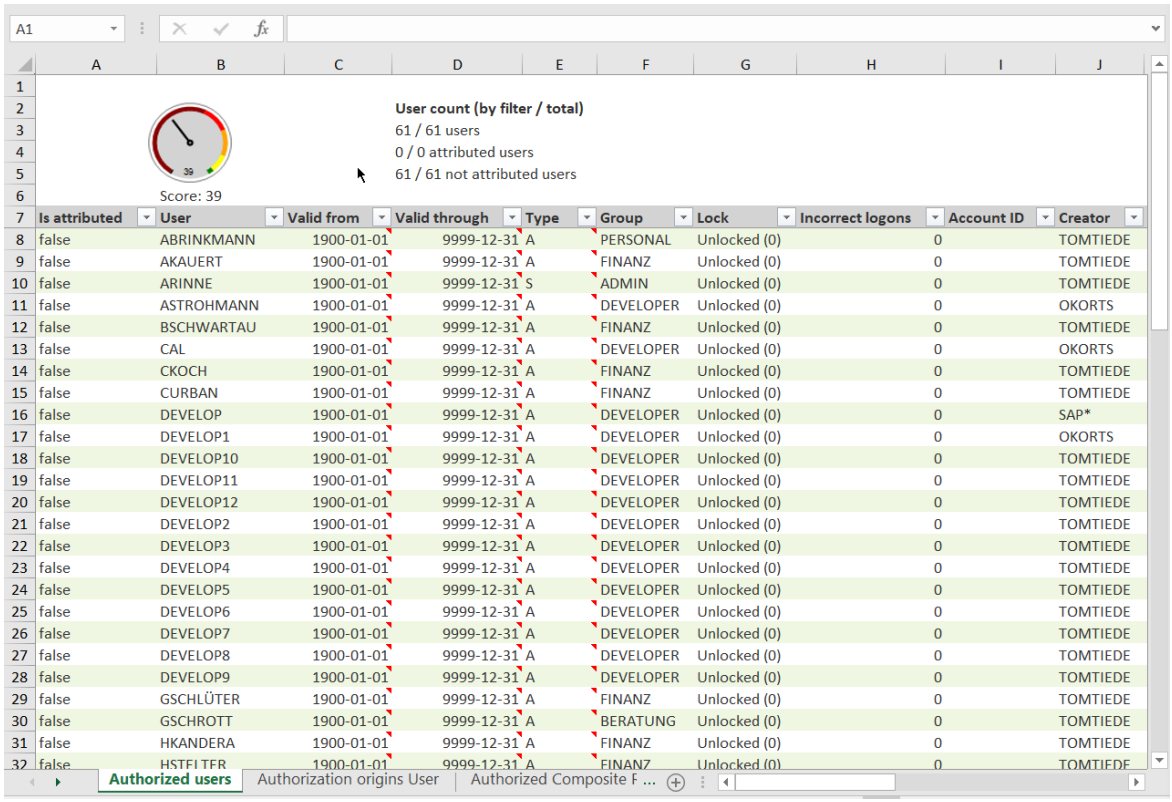



**Figure 187 - Specifying the storage path for the result export**

The result file is created as an Excel workbook (*.xlsx) by default and contains multiple spreadsheets:

| | |
|---|---|
| *Authorized users* | List of authorized users |
| *Authorization origins user* | List of authorized users and the origins of their authorizations |
| *Authorized composite roles* | List of composite roles that fully grant the authorization, origin of authorization |
| *Composite roles* | List of the authorized composites roles with the composite/single roles or authorization objects contained |
| *Authorized single roles* | List of single roles that fully grant the authorization, origin of authorization |
| *Single roles* | List of the authorized single roles with the authorization objects contained |
| *Query* | Technical composition of the authorization query |
| *Analysis settings* | Overview of the check settings |
| *User attribution* | List of legitimate users for this query |
| *Risk Management* | Settings for this query from Risk Management |

| *Documentation* | Information from the documentation for this query |
|---|---|



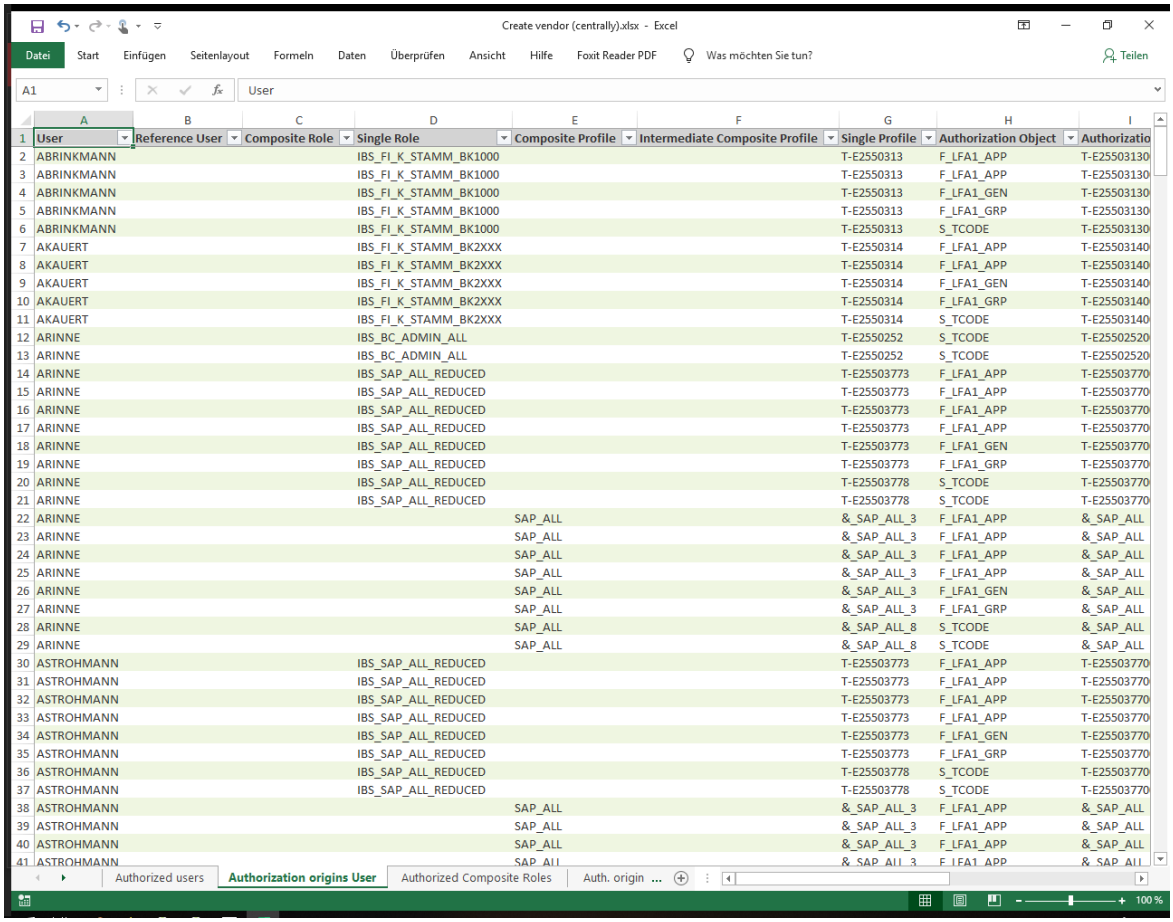
User count (by filter / total)
61 / 61 users
0 / 0 attributed users
61 / 61 not attributed users

Score: 39

| Is attributed | User | Valid from | Valid through | Type | Group | Lock | Incorrect logons | Account ID | Creator |
|---|---|---|---|---|---|---|---|---|---|
| false | ABRINKMANN | 1900-01-01 | 9999-12-31 | A | PERSONAL | Unlocked (0) | 0 | | TOMTIEDE |
| false | AKAUERT | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |
| false | ARINNE | 1900-01-01 | 9999-12-31 | S | ADMIN | Unlocked (0) | 0 | | TOMTIEDE |
| false | ASTROHMANN | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | OKORTS |
| false | BSCHWARTAU | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |
| false | CAL | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | OKORTS |
| false | CKOCH | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |
| false | CURBAN | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | SAP* |
| false | DEVELOP1 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | OKORTS |
| false | DEVELOP10 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP11 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP12 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP2 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP3 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP4 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP5 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP6 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP7 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP8 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | DEVELOP9 | 1900-01-01 | 9999-12-31 | A | DEVELOPER | Unlocked (0) | 0 | | TOMTIEDE |
| false | GSCHLÜTER | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |
| false | GSCHROTT | 1900-01-01 | 9999-12-31 | A | BERATUNG | Unlocked (0) | 0 | | TOMTIEDE |
| false | HKANDERA | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |
| false | HSTELTER | 1900-01-01 | 9999-12-31 | A | FINANZ | Unlocked (0) | 0 | | TOMTIEDE |



**Figure 188 - Result table: List of authorized users**




| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | User | Reference User | Composite Role | Single Role | Composite Profile | Intermediate Composite Profile | Single Profile | Authorization Object | Authorizatio |
| 2 | ABRINKMANN | | | IBS_FI_K_STAMM_BK1000 | | | T-E2550313 | F_LFA1_APP | T-E25503130 |
| 3 | ABRINKMANN | | | IBS_FI_K_STAMM_BK1000 | | | T-E2550313 | F_LFA1_APP | T-E25503130 |
| 4 | ABRINKMANN | | | IBS_FI_K_STAMM_BK1000 | | | T-E2550313 | F_LFA1_GEN | T-E25503130 |
| 5 | ABRINKMANN | | | IBS_FI_K_STAMM_BK1000 | | | T-E2550313 | F_LFA1_GRP | T-E25503130 |
| 6 | ABRINKMANN | | | IBS_FI_K_STAMM_BK1000 | | | T-E2550313 | S_TCODE | T-E25503130 |
| 7 | AKAUERT | | | IBS_FI_K_STAMM_BK2XXX | | | T-E2550314 | F_LFA1_APP | T-E25503140 |
| 8 | AKAUERT | | | IBS_FI_K_STAMM_BK2XXX | | | T-E2550314 | F_LFA1_APP | T-E25503140 |
| 9 | AKAUERT | | | IBS_FI_K_STAMM_BK2XXX | | | T-E2550314 | F_LFA1_GEN | T-E25503140 |
| 10 | AKAUERT | | | IBS_FI_K_STAMM_BK2XXX | | | T-E2550314 | F_LFA1_GRP | T-E25503140 |
| 11 | AKAUERT | | | IBS_FI_K_STAMM_BK2XXX | | | T-E2550314 | S_TCODE | T-E25503140 |
| 12 | ARINNE | | | IBS_BC_ADMIN_ALL | | | T-E2550252 | S_TCODE | T-E25502520 |
| 13 | ARINNE | | | IBS_BC_ADMIN_ALL | | | T-E2550252 | S_TCODE | T-E25502520 |
| 14 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 15 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 16 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 17 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 18 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GEN | T-E25503770 |
| 19 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GRP | T-E25503770 |
| 20 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 21 | ARINNE | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 22 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 23 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 24 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 25 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 26 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_GEN | &_SAP_ALL |
| 27 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_GRP | &_SAP_ALL |
| 28 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_8 | S_TCODE | &_SAP_ALL |
| 29 | ARINNE | | | | SAP_ALL | | &_SAP_ALL_8 | S_TCODE | &_SAP_ALL |
| 30 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 31 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 32 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 33 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 34 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GEN | T-E25503770 |
| 35 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GRP | T-E25503770 |
| 36 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 37 | ASTROHMANN | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 38 | ASTROHMANN | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 39 | ASTROHMANN | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 40 | ASTROHMANN | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 41 | ASTROHMANN | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |

**Figure 189 - Result table: List of authorized users and the origins of their authorizations**

## III - 5.2 Exporting an authorization query - compairing snapshots

If you have selected a second snapshot for comparison for the evaluation of an authorization, the comparison results are included as an additional table in the Excel export:

| Comparison | Is attributed | User | Valid from | Valid through | Type | Group |
|---|---|---|---|---|---|---|
| Previously authorized and deleted | - | JHERRMANN | 1900-01-01 | 9999-12-31 | A | |
| Unchaged | false | JLERCH | 1900-01-01 | 9999-12-31 | A | |
| Newly authorized | false | TEST2 | 1900-01-01 | 9999-12-31 | A | |
| Previously authorized | - | TOMTIEDE | 1900-01-01 | 9999-12-31 | S | SUPER |
| Unchaged | false | WF-BATCH | 1900-01-01 | 9999-12-31 | B | SUPER |

**Figure 190 - Result table: Comparison of two snapshots**

If the snapshots to be compared have different SAP system release levels or changed customizing settings, the authorization query in question may be evaluated with a different definition. This is the case for release-independent authorization queries (authorization queries that are evaluated with different object compositions/definitions based on the SAP system release). For more information, see the chapter *Release-Independent Authorization Queries*. This is displayed as follows on the Query tab in the export:

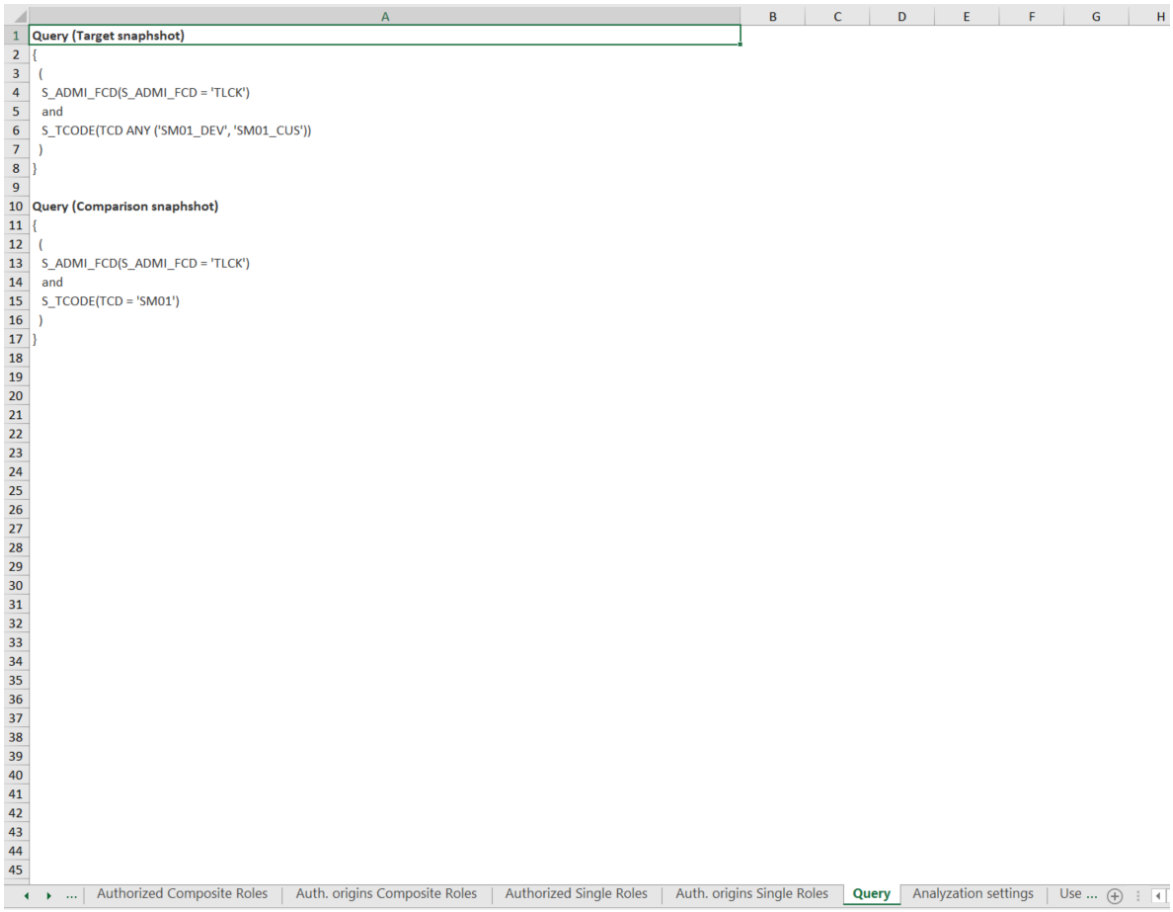



**Figure 191 - Query display in the export: Comparison of two snapshots**

## III - 5.3 Exporting a table query

A table query must be evaluated and selected for the result export. You use the button to start the export. A dialog box for selecting the storage path appears. The result file is created as an Excel workbook (*.xlsx) by default and contains multiple spreadsheets:

| | |
|---|---|
| *Results* | List of the results of the table query |
| *Query* | Technical display of the table query, list of tables, table fields and select and join criteria |
| *Analysation settings* | Overview of the check settings |
| *Assessment* | Display of the criteria for assessing the content of the table queries (requirements fulfilled/not fulfilled) |
| *Documentation* | Information from the documentation for this query |

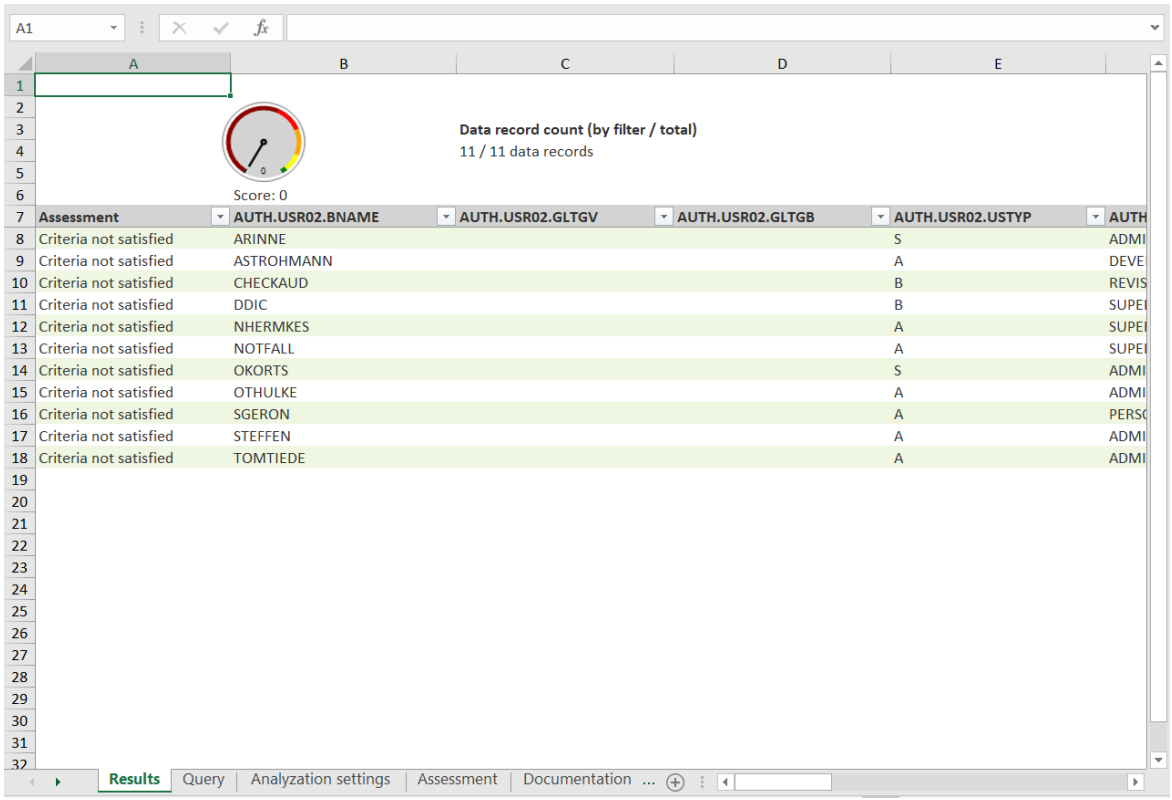
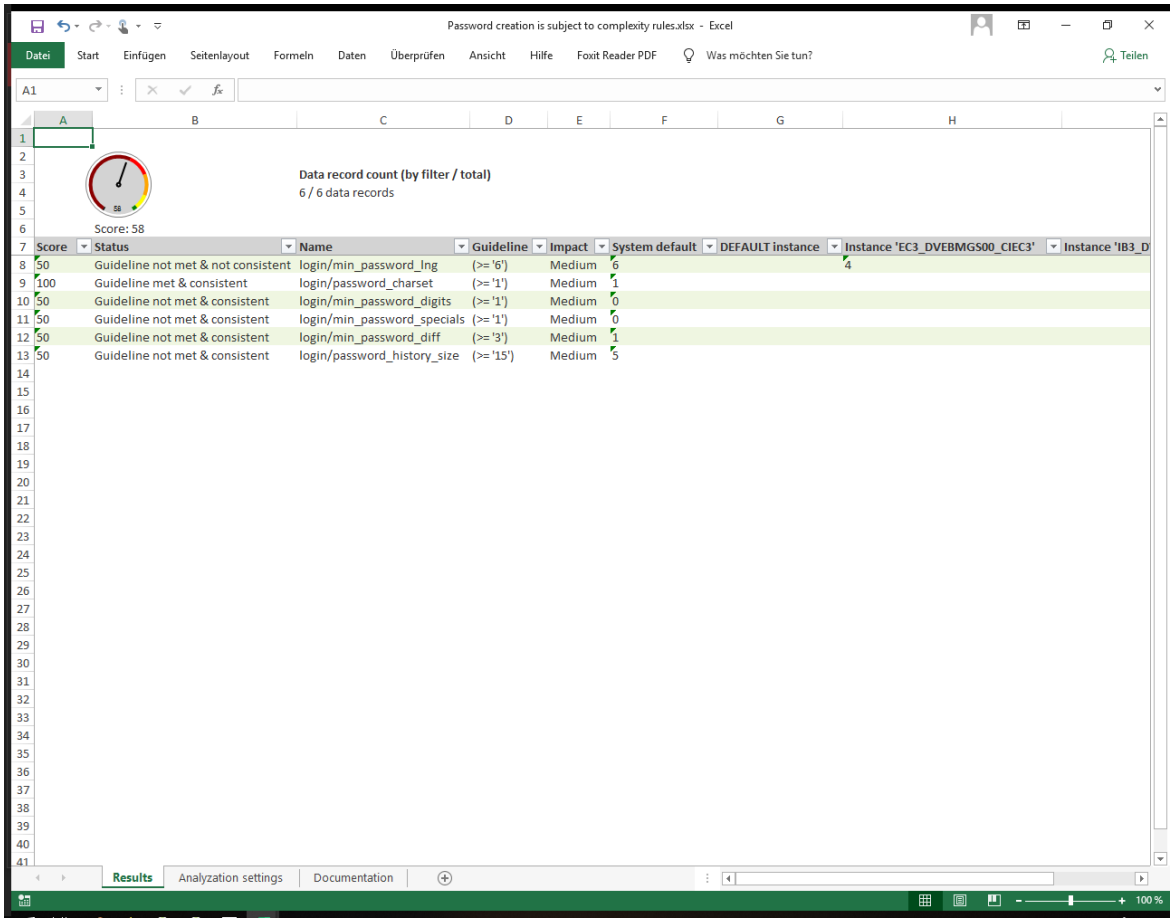



**Figure 192 - Exporting a table query**

## III - 5.4 Exporting a parameter query

A parameter query must be evaluated and selected for the result export. You use the button to start the export. A dialog box for selecting the storage path appears. The result file is created as an Excel workbook (*.xlsx) by default and contains multiple spreadsheets:

| | |
|---|---|
| *Results* | List of the results of the parameter query |
| *Analysation settings* | Overview of the check settings |
| *Documentation* | Information from the documentation for this query |




| Score | Status | Name | Guideline | Impact | System default | DEFAULT instance | Instance 'EC3_DVEBMGS00_CIEC3' | Instance 'IB3_D |
|---|---|---|---|---|---|---|---|---|
| 50 | Guideline not met & not consistent | login/min_password_lng | (>= '6') | Medium | 6 | | 4 | |
| 100 | Guideline met & consistent | login/password_charset | (>= '1') | Medium | 1 | | | |
| 50 | Guideline not met & consistent | login/min_password_digits | (>= '1') | Medium | 0 | | | |
| 50 | Guideline not met & consistent | login/min_password_specials | (>= '1') | Medium | 0 | | | |
| 50 | Guideline not met & consistent | login/min_password_diff | (>= '3') | Medium | 1 | | | |
| 50 | Guideline not met & consistent | login/password_history_size | (>= '15') | Medium | 5 | | | |

**Figure 193 - Exporting a parameter query**

## III - 5.5 Partial / Whole export of an analysis project

You can also perform a partial or full export of the analysis project with multiple authorization queries using the button. To do so, you must first select a subtree in the analysis project or the overall project itself together with multiple evaluated queries:

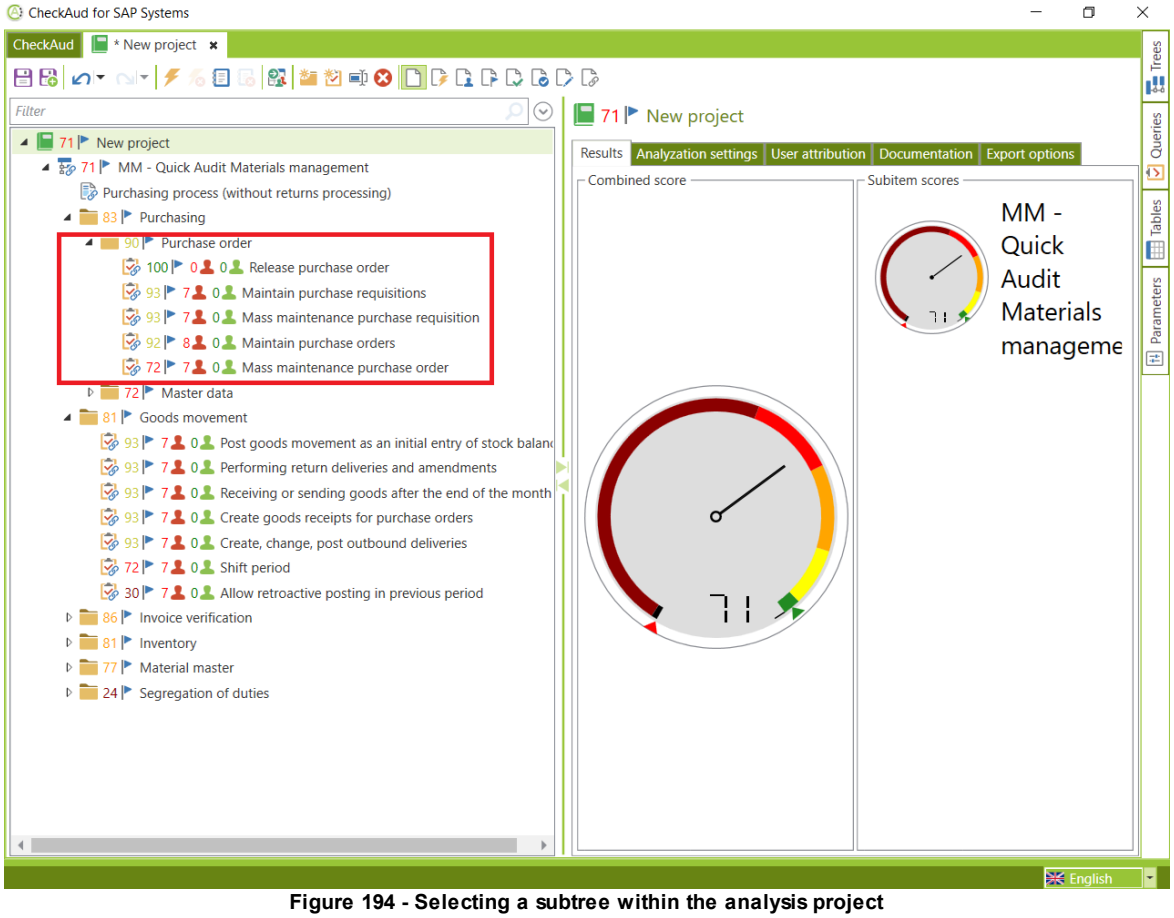



**Figure 194 - Selecting a subtree within the analysis project**

If you now click the button for the export, the standard dialog window for specifying the storage path opens again:

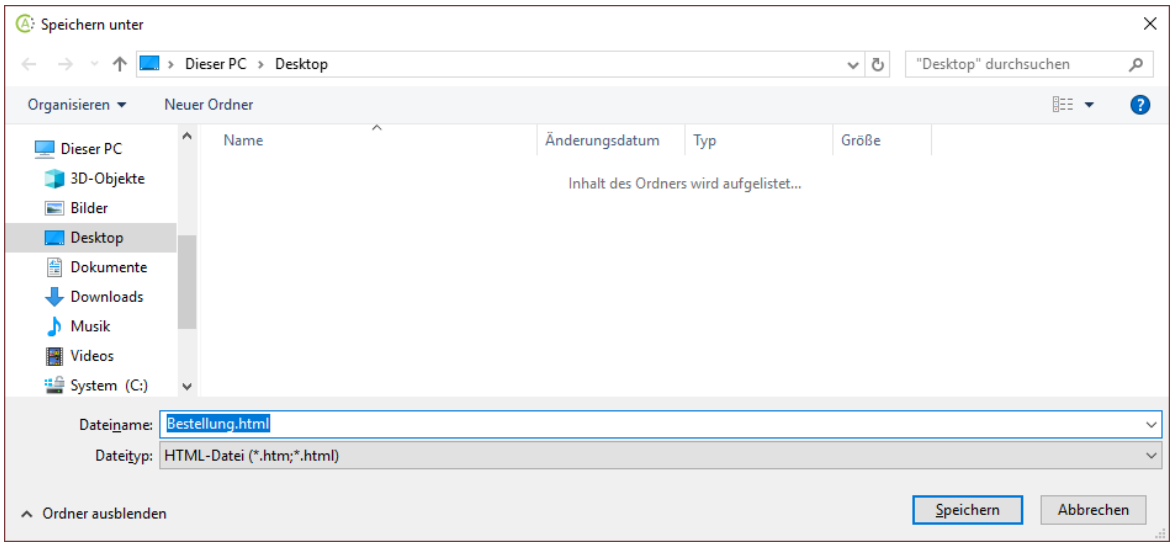



**Figure 195 - Dialog window for storing the partial export**

Unlike the export of an individual query, HTML is specified as the file format for partial or full exports. An HTML overview page is generated and a subdirectory with the individual Excel documents for

each query included in the partial export is automatically created in the same storage location. In the HTML overview, links to this storage location are then set so that you can conveniently open your desired export from the familiar analysis project structure.

You can use the generated HTML overview to select the individual result exports:

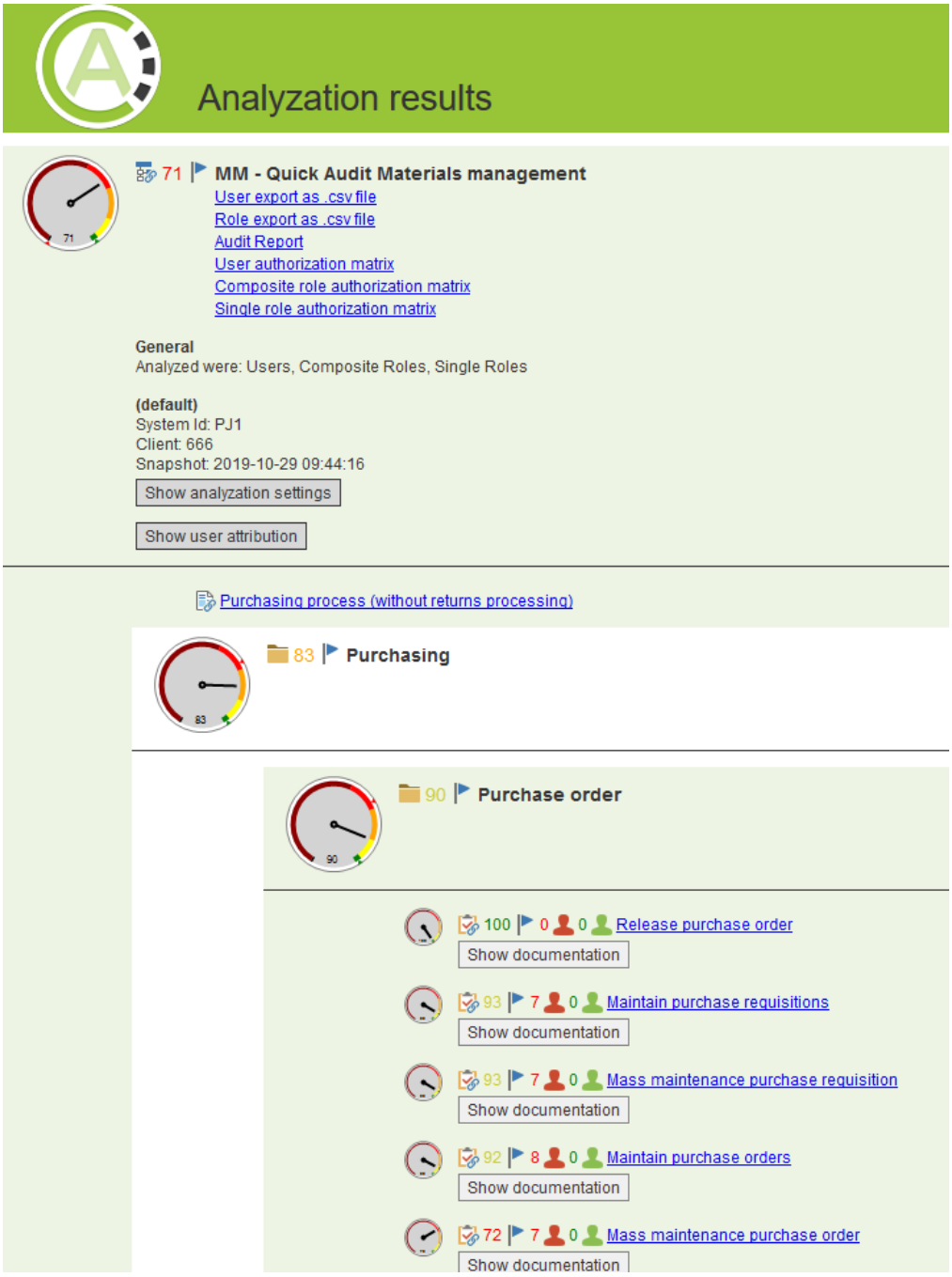



**Figure 196 - HTML overview of a partial export**

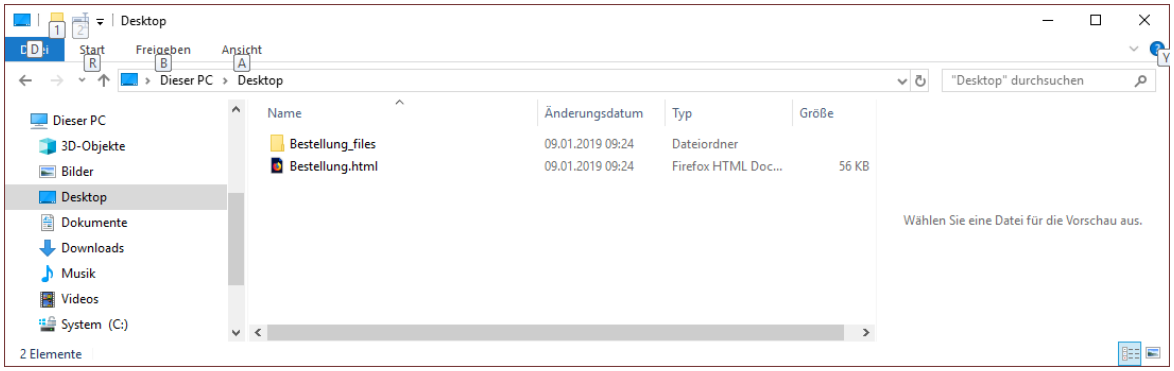



**Figure 197 - Storing the export in the file system**

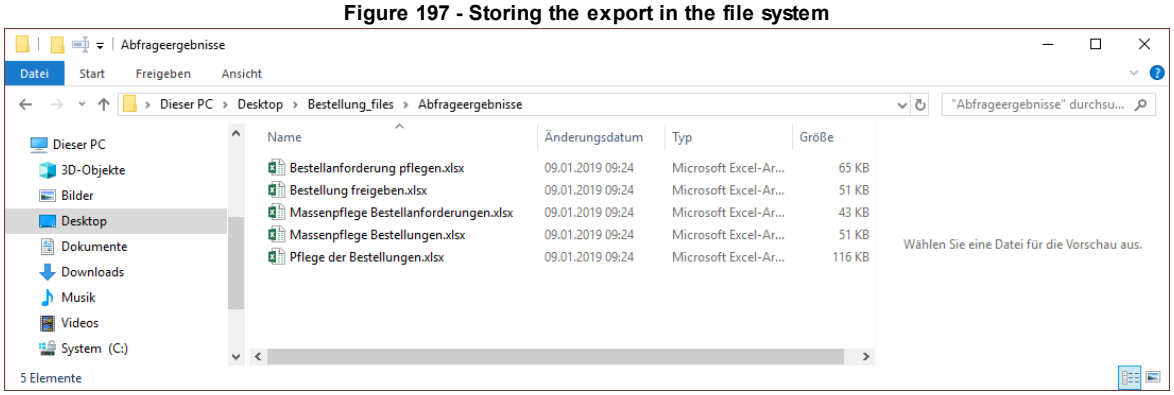



**Figure 198 - Storing the export in the file system**

During the partial or full export, additional composite exports are generated that aggregate multiple individual exports. You can access them from the HTML view:

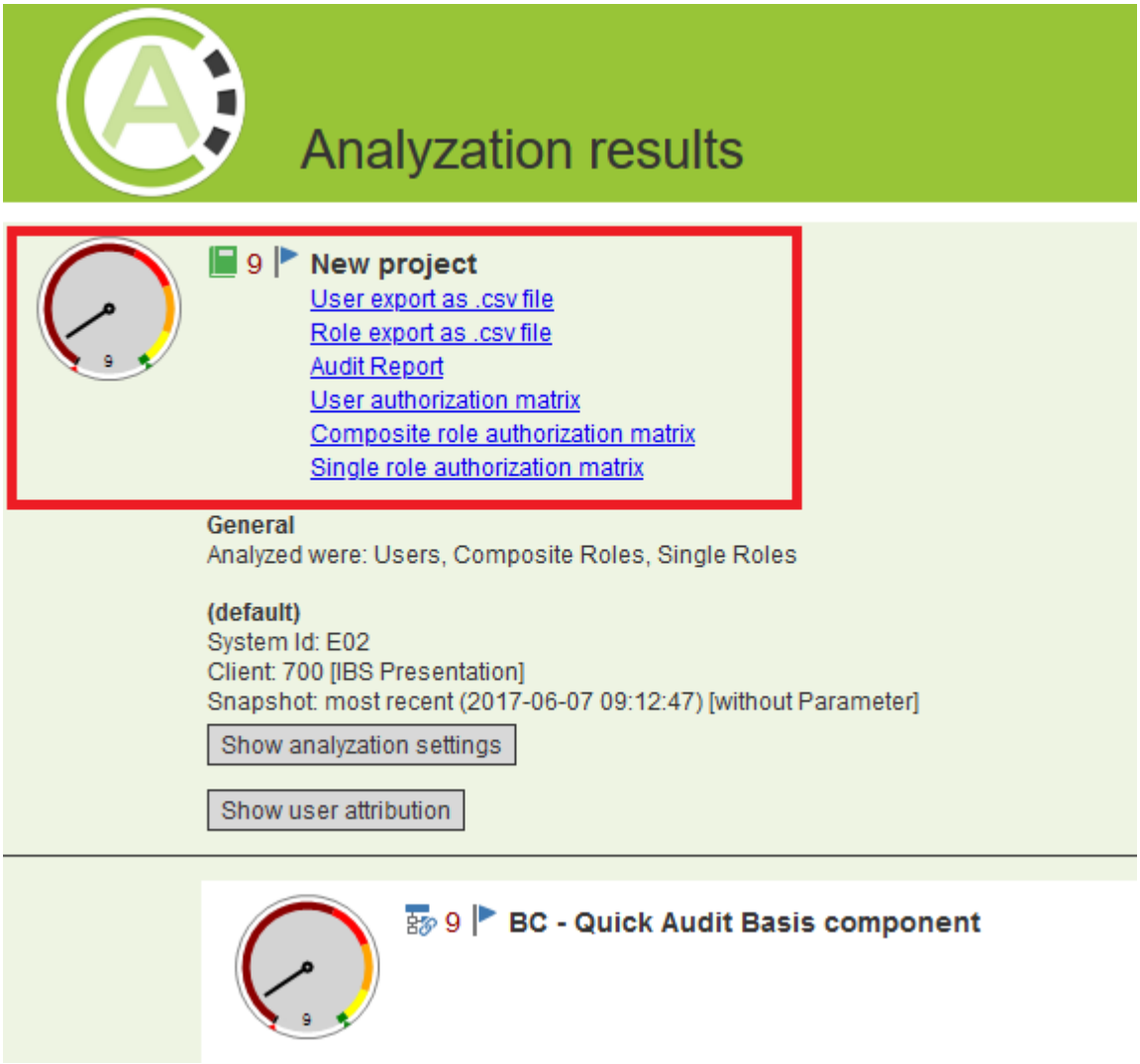
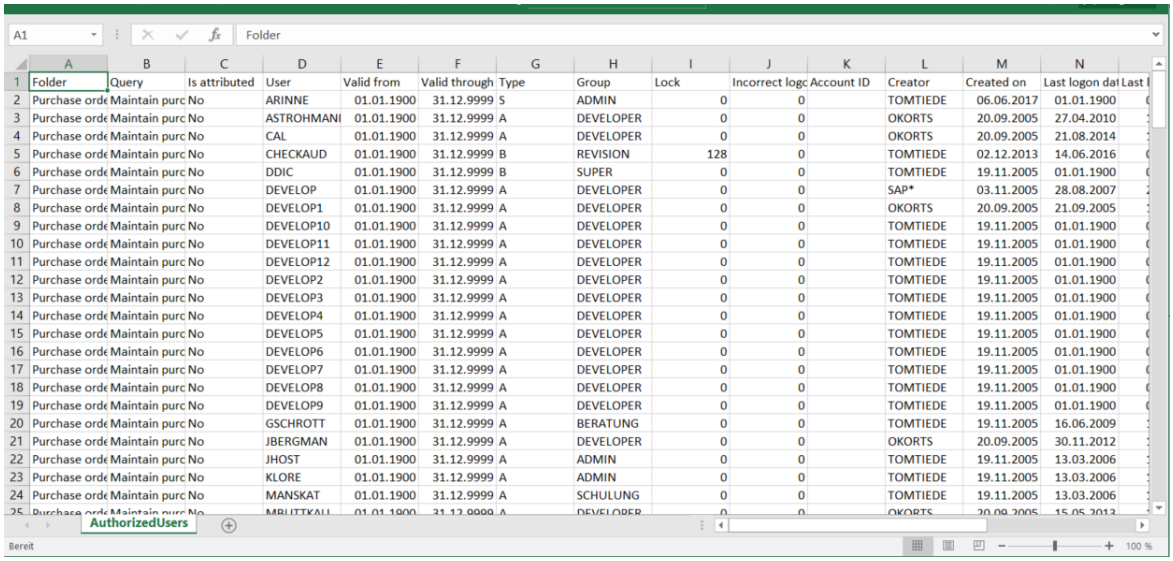



**Figure 199 - Overview of composite exports**

The following composite exports are generated:

| | |
|---|---|
| *User export (csv-file)* | List of all the evaluated authorization queries together with all the authorized users |
| *Role export (csv-file)* | List of all the evaluated authorization queries together with all the authorized roles (composite and single roles) |
| *Audit report (docx-file)* | Results as a formatted Word report |
| *User-authorization-matrix (xlsx-file)* | Comparison of users to authorizations |
| *Single-role-authorization-matrix x (xlsx-file)* | Comparison of single roles to authorizations |
| *Composite-role-authorization-matrix (xlsx-file)* | Comparison of composite roles to authorizations |

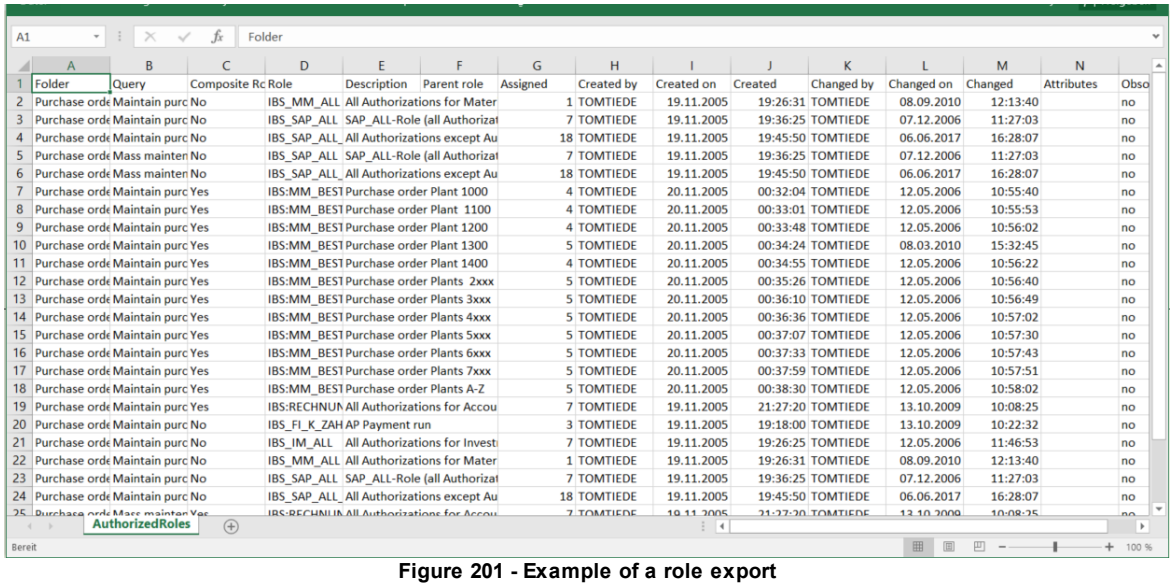
### III - 5.5.1 User export - csv



| Folder | Query | Is attributed | User | Valid from | Valid through | Type | Group | Lock | Incorrect logc | Account ID | Creator | Created on | Last logon dat |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Purchase orde | Maintain purc | No | ARINNE | 01.01.1900 | 31.12.9999 | S | ADMIN | 0 | 0 | | TOMTIEDE | 06.06.2017 | 01.01.1900 |
| Purchase orde | Maintain purc | No | ASTROHMANI | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | OKORTS | 20.09.2005 | 27.04.2010 |
| Purchase orde | Maintain purc | No | CAL | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | OKORTS | 20.09.2005 | 21.08.2014 |
| Purchase orde | Maintain purc | No | CHECKAUD | 01.01.1900 | 31.12.9999 | B | REVISION | 128 | 0 | | TOMTIEDE | 02.12.2013 | 14.06.2016 |
| Purchase orde | Maintain purc | No | DDIC | 01.01.1900 | 31.12.9999 | B | SUPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | SAP* | 03.11.2005 | 28.08.2007 |
| Purchase orde | Maintain purc | No | DEVELOP1 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | OKORTS | 20.09.2005 | 21.09.2005 |
| Purchase orde | Maintain purc | No | DEVELOP10 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP11 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP12 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP2 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP3 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP4 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP5 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP6 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP7 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP8 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | DEVELOP9 | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | TOMTIEDE | 19.11.2005 | 01.01.1900 |
| Purchase orde | Maintain purc | No | GSCHROTT | 01.01.1900 | 31.12.9999 | A | BERATUNG | 0 | 0 | | TOMTIEDE | 19.11.2005 | 16.06.2009 |
| Purchase orde | Maintain purc | No | JBERGMAN | 01.01.1900 | 31.12.9999 | A | DEVELOPER | 0 | 0 | | OKORTS | 20.09.2005 | 30.11.2012 |
| Purchase orde | Maintain purc | No | JHOST | 01.01.1900 | 31.12.9999 | A | ADMIN | 0 | 0 | | TOMTIEDE | 19.11.2005 | 13.03.2006 |
| Purchase orde | Maintain purc | No | KLORE | 01.01.1900 | 31.12.9999 | A | ADMIN | 0 | 0 | | TOMTIEDE | 19.11.2005 | 13.03.2006 |
| Purchase orde | Maintain purc | No | MANSKAT | 01.01.1900 | 31.12.9999 | A | SCHULUNG | 0 | 0 | | TOMTIEDE | 19.11.2005 | 13.03.2006 |

Figure 200 - Example of a user export

### III - 5.5.2 Role export - csv



| Folder | Query | Composite Rc | Role | Description | Parent role | Assigned | Created by | Created on | Created | Changed by | Changed on | Changed | Attributes | Obso |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Purchase orde | Maintain purc | No | IBS_MM_ALL | All Authorizations for Mater | | 1 | TOMTIEDE | 19.11.2005 | 19:26:31 | TOMTIEDE | 08.09.2010 | 12:13:40 | | no |
| Purchase orde | Maintain purc | No | IBS_SAP_ALL | SAP_ALL-Role (all Authorizat | | 7 | TOMTIEDE | 19.11.2005 | 19:36:25 | TOMTIEDE | 07.12.2006 | 11:27:03 | | no |
| Purchase orde | Maintain purc | No | IBS_SAP_ALL_ | All Authorizations except Au | | 18 | TOMTIEDE | 19.11.2005 | 19:45:50 | TOMTIEDE | 06.06.2017 | 16:28:07 | | no |
| Purchase orde | Mass mainten | No | IBS_SAP_ALL | SAP_ALL-Role (all Authorizat | | 7 | TOMTIEDE | 19.11.2005 | 19:36:25 | TOMTIEDE | 07.12.2006 | 11:27:03 | | no |
| Purchase orde | Mass mainten | No | IBS_SAP_ALL_ | All Authorizations except Au | | 18 | TOMTIEDE | 19.11.2005 | 19:45:50 | TOMTIEDE | 06.06.2017 | 16:28:07 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plant 1000 | | 4 | TOMTIEDE | 20.11.2005 | 00:32:04 | TOMTIEDE | 12.05.2006 | 10:55:40 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plant 1100 | | 4 | TOMTIEDE | 20.11.2005 | 00:33:01 | TOMTIEDE | 12.05.2006 | 10:55:53 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plant 1200 | | 4 | TOMTIEDE | 20.11.2005 | 00:33:48 | TOMTIEDE | 12.05.2006 | 10:56:02 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plant 1300 | | 5 | TOMTIEDE | 20.11.2005 | 00:34:24 | TOMTIEDE | 08.03.2010 | 15:32:45 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plant 1400 | | 4 | TOMTIEDE | 20.11.2005 | 00:34:55 | TOMTIEDE | 12.05.2006 | 10:56:22 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants 2xxx | | 5 | TOMTIEDE | 20.11.2005 | 00:35:26 | TOMTIEDE | 12.05.2006 | 10:56:40 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants 3xxx | | 5 | TOMTIEDE | 20.11.2005 | 00:36:10 | TOMTIEDE | 12.05.2006 | 10:56:49 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants 4xxx | | 5 | TOMTIEDE | 20.11.2005 | 00:36:36 | TOMTIEDE | 12.05.2006 | 10:57:02 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants 5xxx | | 5 | TOMTIEDE | 20.11.2005 | 00:37:07 | TOMTIEDE | 12.05.2006 | 10:57:30 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants 6xxx | | 5 | TOMTIEDE | 20.11.2005 | 00:37:33 | TOMTIEDE | 12.05.2006 | 10:57:43 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants 7xxx | | 5 | TOMTIEDE | 20.11.2005 | 00:37:59 | TOMTIEDE | 12.05.2006 | 10:57:51 | | no |
| Purchase orde | Maintain purc | Yes | IBS:MM_BEST | Purchase order Plants A-Z | | 5 | TOMTIEDE | 20.11.2005 | 00:38:30 | TOMTIEDE | 12.05.2006 | 10:58:02 | | no |
| Purchase orde | Maintain purc | Yes | IBS:RECHNUN | All Authorizations for Accou | | 7 | TOMTIEDE | 19.11.2005 | 21:27:20 | TOMTIEDE | 13.10.2009 | 10:08:25 | | no |
| Purchase orde | Maintain purc | No | IBS_FI_K_ZAH | AP Payment run | | 3 | TOMTIEDE | 19.11.2005 | 19:18:00 | TOMTIEDE | 13.10.2009 | 10:22:32 | | no |
| Purchase orde | Maintain purc | No | IBS_IM_ALL | All Authorizations for Investi | | 7 | TOMTIEDE | 19.11.2005 | 19:26:25 | TOMTIEDE | 12.05.2006 | 11:46:53 | | no |
| Purchase orde | Maintain purc | No | IBS_MM_ALL | All Authorizations for Mater | | 1 | TOMTIEDE | 19.11.2005 | 19:26:31 | TOMTIEDE | 08.09.2010 | 12:13:40 | | no |
| Purchase orde | Maintain purc | No | IBS_SAP_ALL | SAP_ALL-Role (all Authorizat | | 7 | TOMTIEDE | 19.11.2005 | 19:36:25 | TOMTIEDE | 07.12.2006 | 11:27:03 | | no |
| Purchase orde | Maintain purc | No | IBS_SAP_ALL_ | All Authorizations except Au | | 18 | TOMTIEDE | 19.11.2005 | 19:45:50 | TOMTIEDE | 06.06.2017 | 16:28:07 | | no |

Figure 201 - Example of a role export

## III - 5.5.3 Audit report - docx

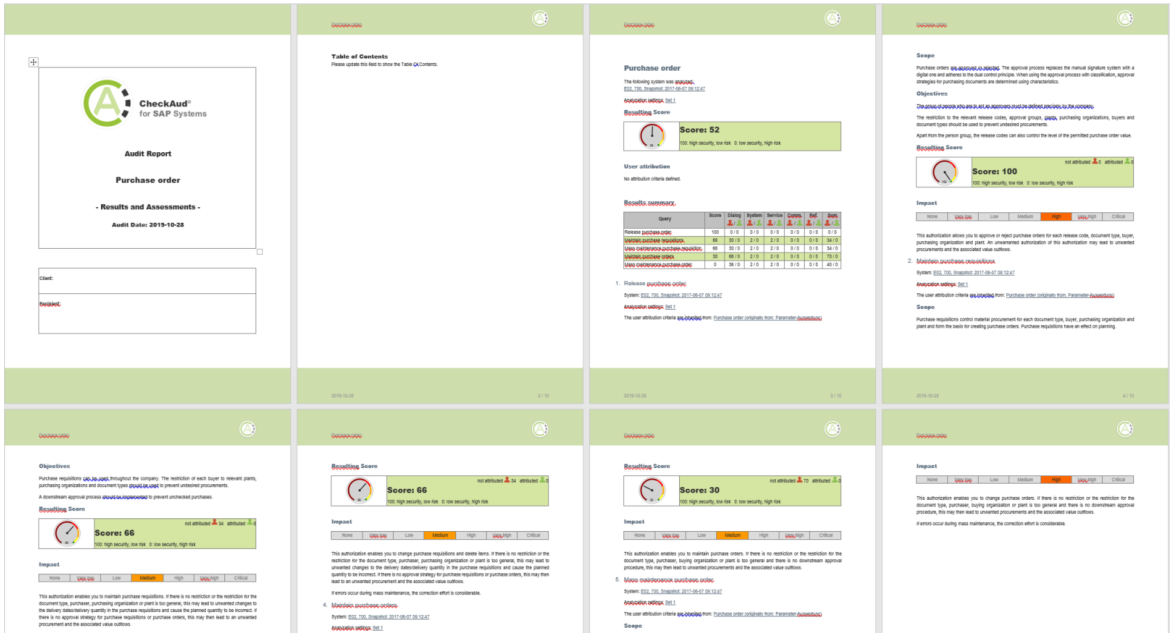



Figure 202 - Example of a audit report

## III - 5.5.4 User-authorization-matrix - xlsx

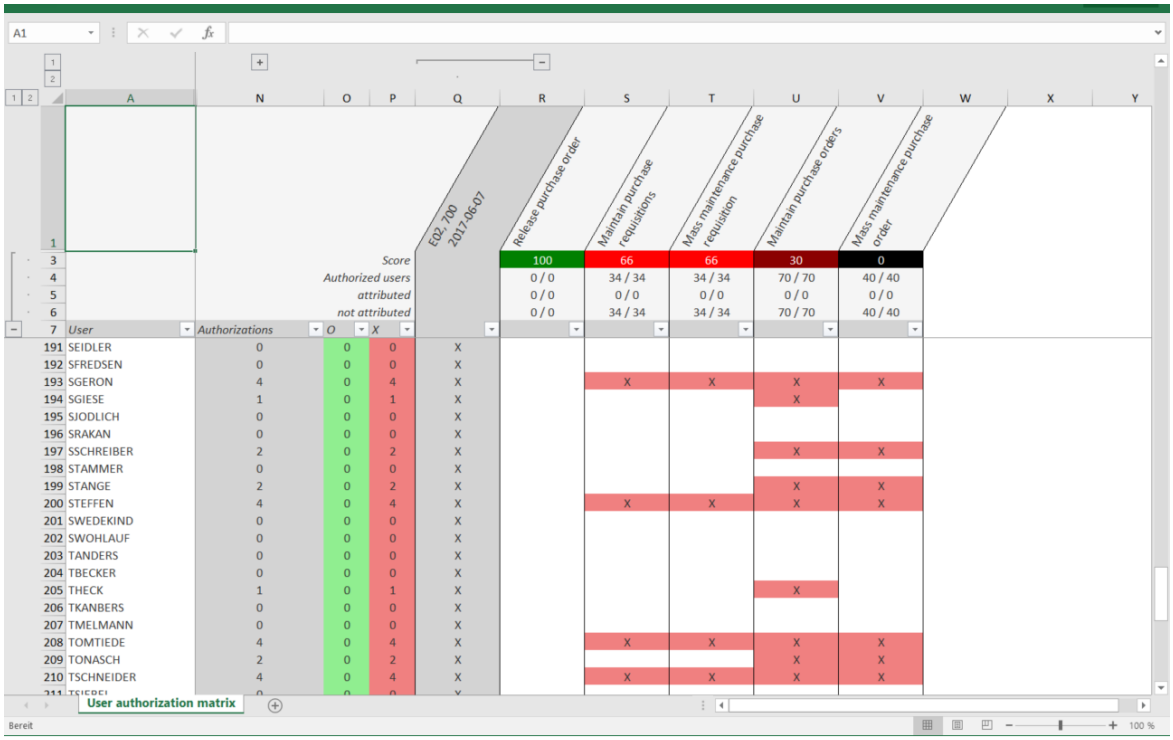
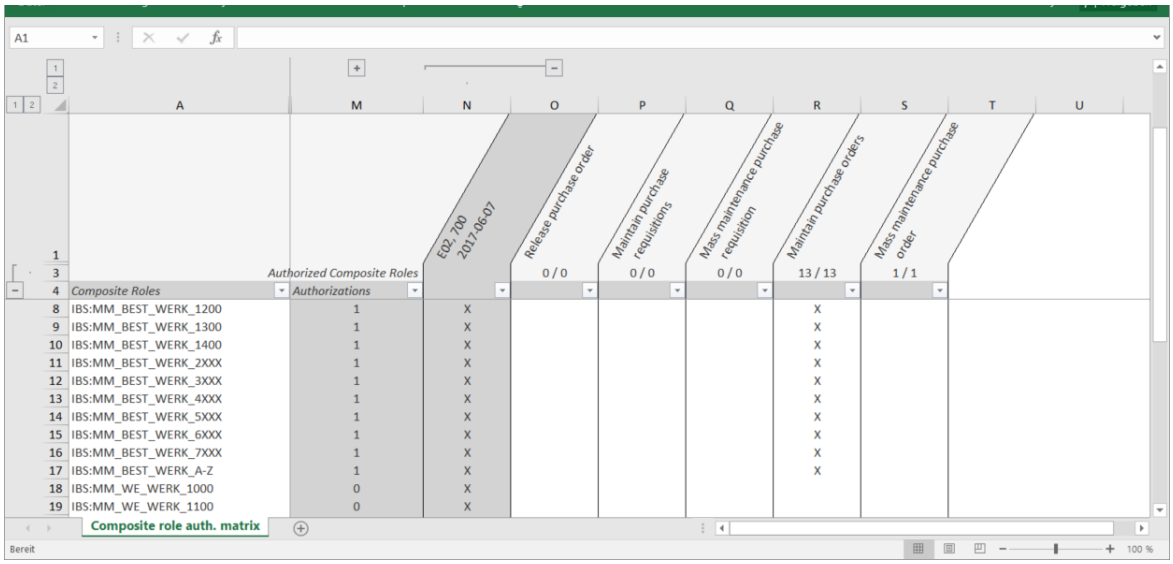



Figure 203 - Example of a user-authorization-matrix

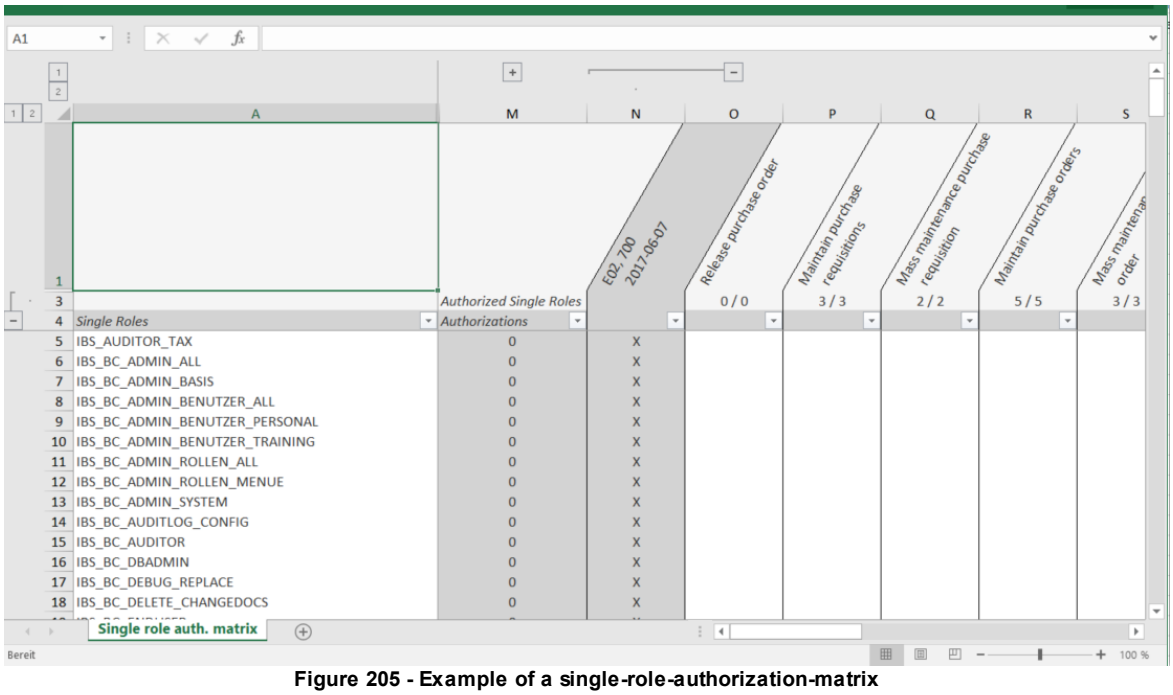
### III - 5.5.5 Composite-role-authorization-matrix - xls



| | A | M | N | O | P | Q | R | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | E02, 700 2017-06-07 | Release purchase order | Maintain purchase requisitions | Mass maintenance purchase requisition | Maintain purchase orders | Mass maintenance purchase order | | |
| 3 | | Authorized Composite Roles | | 0 / 0 | 0 / 0 | 0 / 0 | 13 / 13 | 1 / 1 | | |
| 4 | Composite Roles | Authorizations | | | | | | | | |
| 8 | IBS:MM_BEST_WERK_1200 | 1 | X | | | | X | | | |
| 9 | IBS:MM_BEST_WERK_1300 | 1 | X | | | | X | | | |
| 10 | IBS:MM_BEST_WERK_1400 | 1 | X | | | | X | | | |
| 11 | IBS:MM_BEST_WERK_2XXX | 1 | X | | | | X | | | |
| 12 | IBS:MM_BEST_WERK_3XXX | 1 | X | | | | X | | | |
| 13 | IBS:MM_BEST_WERK_4XXX | 1 | X | | | | X | | | |
| 14 | IBS:MM_BEST_WERK_5XXX | 1 | X | | | | X | | | |
| 15 | IBS:MM_BEST_WERK_6XXX | 1 | X | | | | X | | | |
| 16 | IBS:MM_BEST_WERK_7XXX | 1 | X | | | | X | | | |
| 17 | IBS:MM_BEST_WERK_A-Z | 1 | X | | | | X | | | |
| 18 | IBS:MM_WE_WERK_1000 | 0 | X | | | | | | | |
| 19 | IBS:MM_WE_WERK_1100 | 0 | X | | | | | | | |

Figure 204 - Example of a composite-role-authorization-matrix

### III - 5.5.6 Single-role-authorization-matrix - xls



| | A | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|
| 1 | | | E02, 700 2017-06-07 | Release purchase order | Maintain purchase requisitions | Mass maintenance purchase requisition | Maintain purchase orders | Mass maintenan order |
| 3 | | Authorized Single Roles | | 0 / 0 | 3 / 3 | 2 / 2 | 5 / 5 | 3 / 3 |
| 4 | Single Roles | Authorizations | | | | | | |
| 5 | IBS_AUDITOR_TAX | 0 | X | | | | | |
| 6 | IBS_BC_ADMIN_ALL | 0 | X | | | | | |
| 7 | IBS_BC_ADMIN_BASIS | 0 | X | | | | | |
| 8 | IBS_BC_ADMIN_BENUTZER_ALL | 0 | X | | | | | |
| 9 | IBS_BC_ADMIN_BENUTZER_PERSONAL | 0 | X | | | | | |
| 10 | IBS_BC_ADMIN_BENUTZER_TRAINING | 0 | X | | | | | |
| 11 | IBS_BC_ADMIN_ROLLEN_ALL | 0 | X | | | | | |
| 12 | IBS_BC_ADMIN_ROLLEN_MENUE | 0 | X | | | | | |
| 13 | IBS_BC_ADMIN_SYSTEM | 0 | X | | | | | |
| 14 | IBS_BC_AUDITLOG_CONFIG | 0 | X | | | | | |
| 15 | IBS_BC_AUDITOR | 0 | X | | | | | |
| 16 | IBS_BC_DBADMIN | 0 | X | | | | | |
| 17 | IBS_BC_DEBUG_REPLACE | 0 | X | | | | | |
| 18 | IBS_BC_DELETE_CHANGEDOCS | 0 | X | | | | | |

Figure 205 - Example of a single-role-authorization-matrix

### III - 5.5.7 Exports in a matrix view - linked Excel documents

The matrix view does not show the details of the origins of authorizations for individual users or roles. However, the matrix documents are linked to the detailed individual Excel exports and provide additional information in this way if necessary:

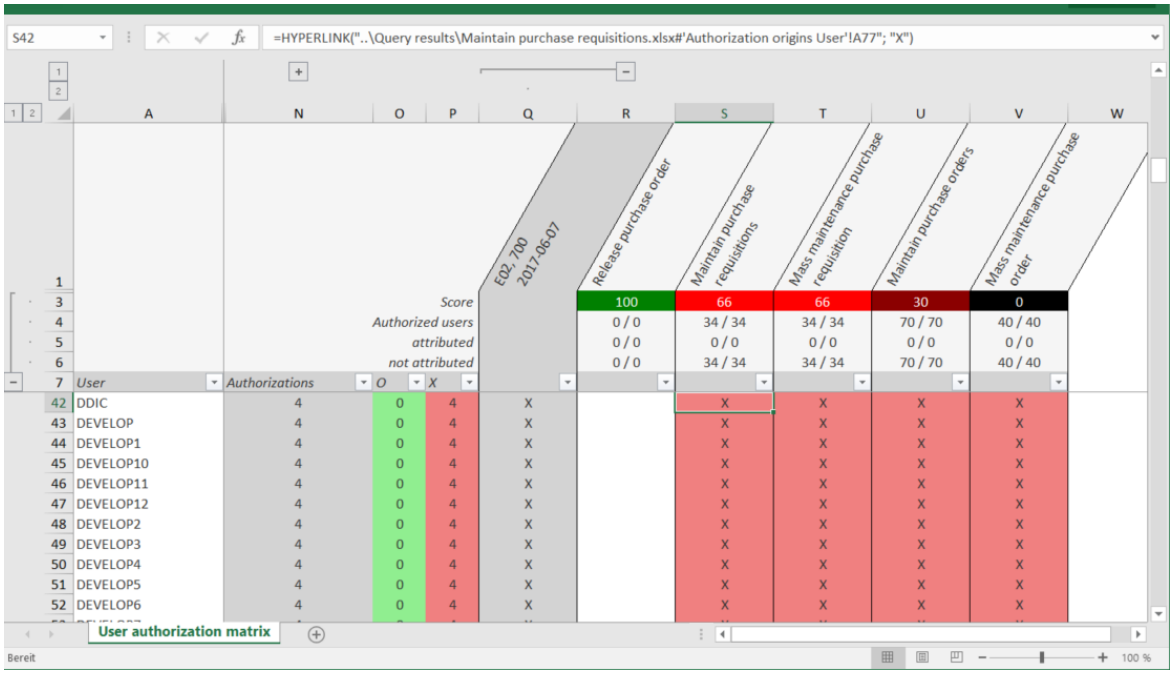
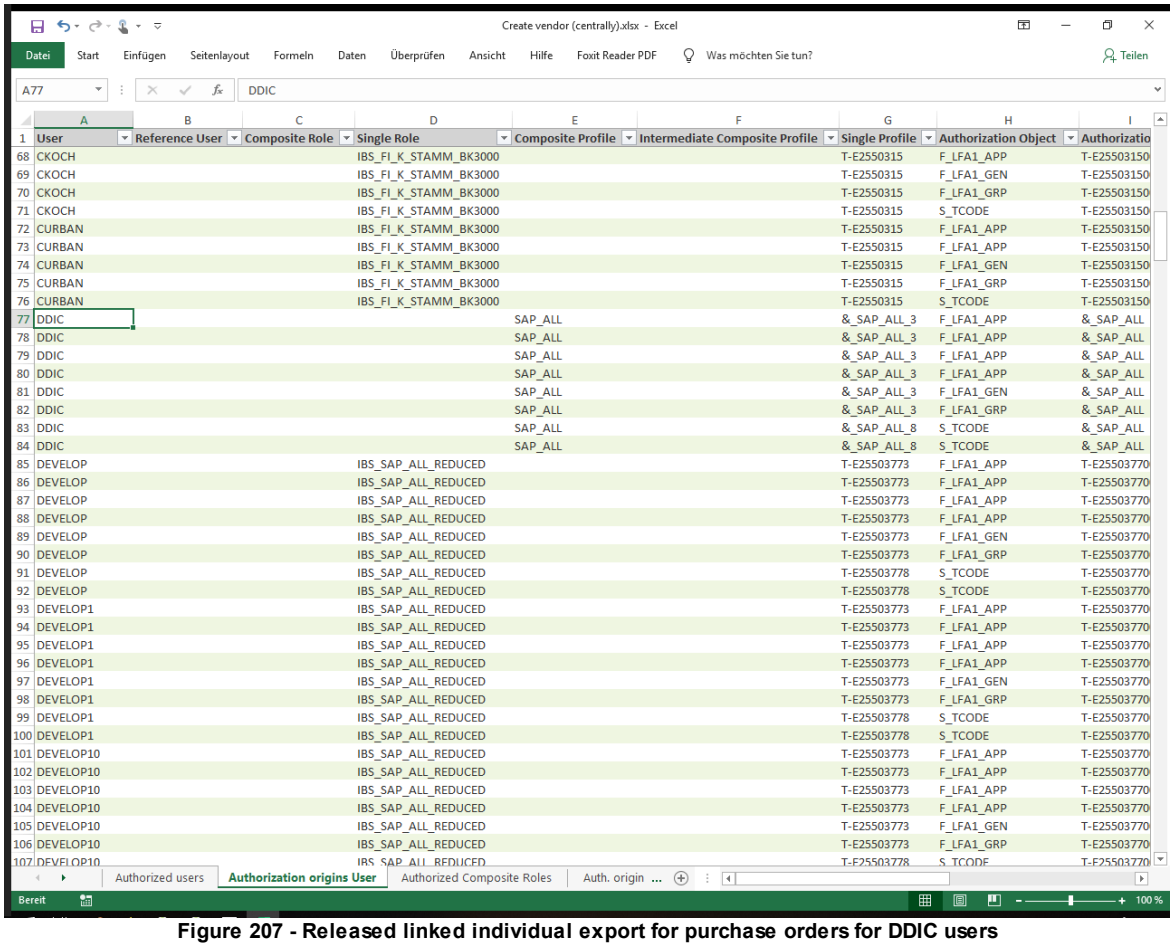



**Figure 206 - User-authorization-matrix**

To open the detailed list of authorization origins for a user (in this example) in the user/authorization matrix, you can select the cell where the user and authorization intersect X by clicking it. The individual export for the authorization in question opens together with the user selected beforehand and the origins of his or her authorizations:




| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | User | Reference User | Composite Role | Single Role | Composite Profile | Intermediate Composite Profile | Single Profile | Authorization Object | Authorizatio |
| 68 | CKOCH | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_APP | T-E25503150 |
| 69 | CKOCH | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_GEN | T-E25503150 |
| 70 | CKOCH | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_GRP | T-E25503150 |
| 71 | CKOCH | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | S_TCODE | T-E25503150 |
| 72 | CURBAN | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_APP | T-E25503150 |
| 73 | CURBAN | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_APP | T-E25503150 |
| 74 | CURBAN | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_GEN | T-E25503150 |
| 75 | CURBAN | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | F_LFA1_GRP | T-E25503150 |
| 76 | CURBAN | | | IBS_FI_K_STAMM_BK3000 | | | T-E2550315 | S_TCODE | T-E25503150 |
| 77 | DDIC | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 78 | DDIC | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 79 | DDIC | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 80 | DDIC | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_APP | &_SAP_ALL |
| 81 | DDIC | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_GEN | &_SAP_ALL |
| 82 | DDIC | | | | SAP_ALL | | &_SAP_ALL_3 | F_LFA1_GRP | &_SAP_ALL |
| 83 | DDIC | | | | SAP_ALL | | &_SAP_ALL_8 | S_TCODE | &_SAP_ALL |
| 84 | DDIC | | | | SAP_ALL | | &_SAP_ALL_8 | S_TCODE | &_SAP_ALL |
| 85 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 86 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 87 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 88 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 89 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GEN | T-E25503770 |
| 90 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GRP | T-E25503770 |
| 91 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 92 | DEVELOP | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 93 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 94 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 95 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 96 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 97 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GEN | T-E25503770 |
| 98 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GRP | T-E25503770 |
| 99 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 100 | DEVELOP1 | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |
| 101 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 102 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 103 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 104 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_APP | T-E25503770 |
| 105 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GEN | T-E25503770 |
| 106 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503773 | F_LFA1_GRP | T-E25503770 |
| 107 | DEVELOP10 | | | IBS_SAP_ALL_REDUCED | | | T-E25503778 | S_TCODE | T-E25503770 |

**Figure 207 - Released linked individual export for purchase orders for DDIC users**

**Note:** This function is also provided in the single-role-matrix and the composite-role-matrix.

## III - 5.6 Encryption of export files

The export of single results will be started with the butten . If necessary, the export files can be encrypted for safe data storage:

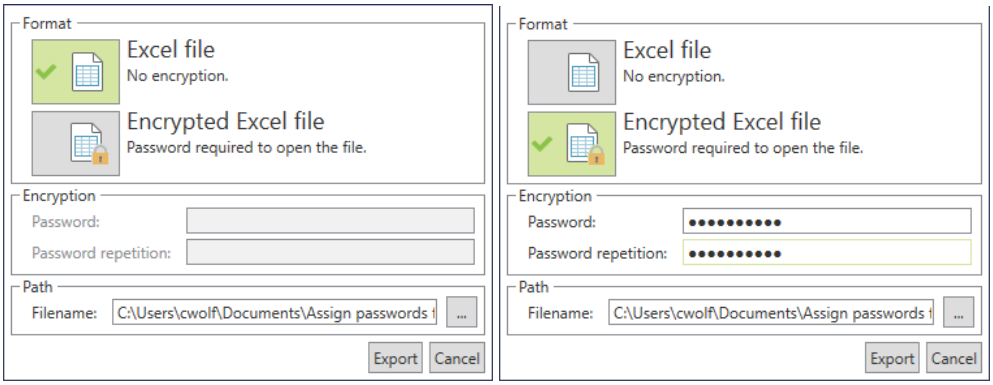



**Figure 208 - Selection for encrypting an export file**

For a paratial or whole result export, there is also a possibility to encrypt the export files. Instead encrypting every single file, a encrypted ZIP archive will be created during this export:

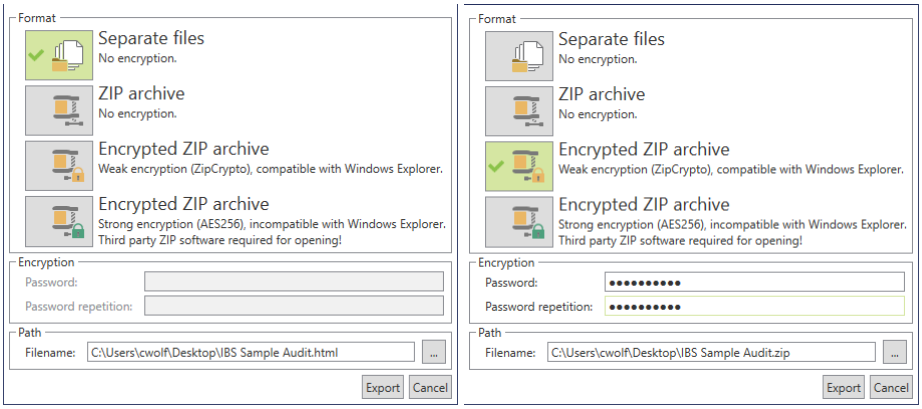



**Figure 209 - Selection for encrypting an export file**

**Note: Encryption of ZIP archives:**

The Windows Explorer compatible *ZipCrypto* encryption computes with the password a 40bit key which is used to encrypt the archive. This procedure is susceptible for simple brute force attacks.

The stronger encryption *AES256* uses block ciphers based on the Rijndael algorithm and is classified as the most used and most safe encryption method. To use this encryption you'll need 3rd-party products. It's advisable to encrypt the exports from CheckAud with the AES256 method and a complex, long password.

## III - 5.7 Displaying the last exported files

After you export results, the most recent exports are listed in chronological order in the lower area of the program window. This allows for convenient and quick access to files that have already been exported.

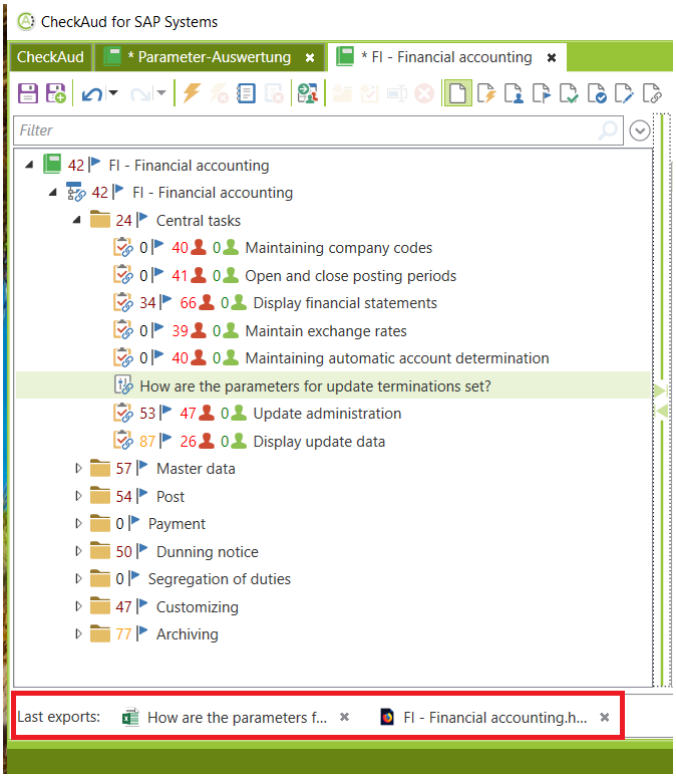



**Figure 210 - Quick access to the last exports performed**

Click the ✖ button next to each export to remove the corresponding quick access items from the view. If necessary, you can close the quick access bar using the ✖ button in the bottom right program window.


**Note:** The list of recently exported results is restricted to the analysis project file that is currently open. When you close the project file, the quick access items displayed beforehand are removed. The saved exports remain available at the storage path.

## III - 5.8 Options for partial/full export

For partial and full exports, you can configure project-specific settings for the individual and composite exports created. To do so, you must select the root of an open analysis project. Display in the Export options tab in the main window:

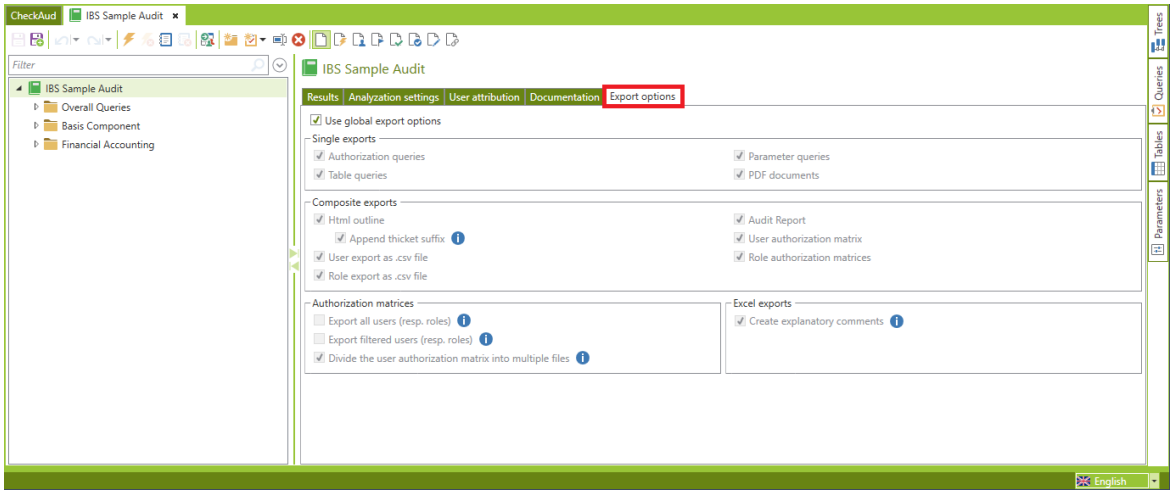



**Figure 211 - Configuring partial/full exports**

*Single exports*:

You can use the individual flags to control which single export files are to be generated during the partial or full export. For example, if you deactivate the Authorization queries flag, then no Excel export files are generated for the evaluated authorizations in the next partial/full export..

*Composite exports*:

You can use the individual flags to control which composite export files are to be generated during the partial or full export. For example, if you deactivate the *Audit report* flag, then no audit reports are generated as Word documents in the next partial/full export.

**Note:** *Thicket directory*
If activated, the "_files" suffix is appended to the name of the export directory. This automatically connects the directory to the corresponding export file (HTML overview). If deactivated, the "_contents" suffix is used instead. This is useful if you do not want the export file and export directory to be connected automatically. You can deactivate this option, for example, if you want to upload the exports to a SharePoint server (the thicket directory would not be visible there).

*Authorization matrices*:

You can use these flags to control how the various authorization matrices (user-authorization-matrix, single-role-authorization-matrix and composite-role-authorization-matrix) are to be structured.

| | |
|---|---|
| *Export all users (or roles)* | If activated, all the analyzed users (or roles) from the SAP system are added to the authorization matrix.<br><br>If deactivated, only users (or roles) that have an entry (authorization) are exported. Users (or roles) without authorizations are excluded. |

| | |
|---|---|
| *Export filtered users (or roles)* | User filters can be set during the analysis. These filters cause some users (or roles) to be excluded from the analysis.<br><br>If activated, the users (or roles) that are filtered out of the analysis are still included in the authorization-matrix (and marked with a " - ").<br><br>If deactivated, the users (or roles) that are filtered out of the analysis are not included in the authorization-matrix. |
| *Divide the user authorization matrix into multiple files* | The user-authorization-matrix is generated as an Excel file. However, since it is difficult to work with very large Excel files, the export is divided into several smaller files by default. The Excel files each contain a maximum of 50,000 data records. If you do not want the file to be divided, you can deactivate this setting here. |
| Add explanatory comments | While generating Excel files, comments can be created that point out specific issues. For instance, not all date information can be displayed in Excel. If the date is converted automatically, an explanatory comment is added to the cell. If you do not require comments, you can deactivate this option. |

**Note:** If you activate the *Use global export options* setting, then the export options from the CheckAud program settings are applied for this open project (see the chapter *Settings*). If you set your own options that differ from the global export options for the open analysis project, you must deactivate the *Use global export options* flag.

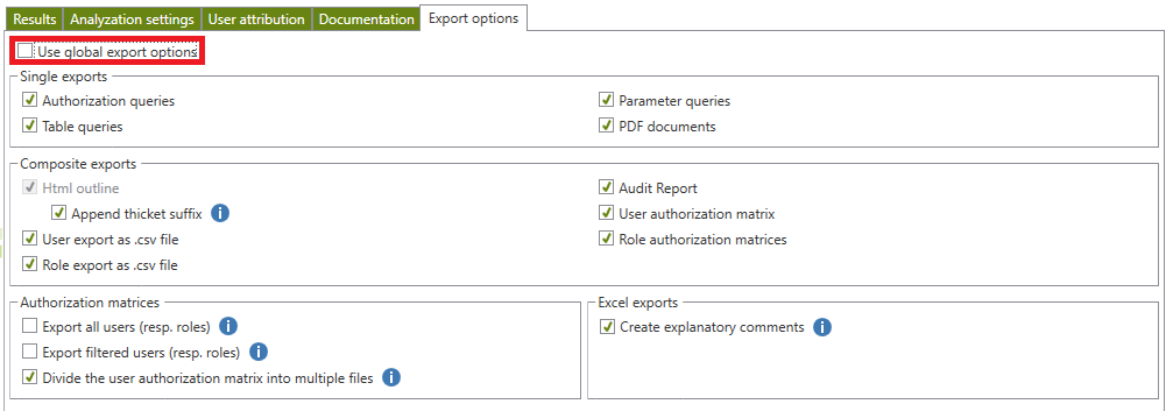



**Figure 212 - Custom configuration for partial/full exports**

If you activate the *Use global export options* flag again, the global program export settings are applied with immediate effect.

Rights origins and query compositions can be found in the settings under Individual exports and Excel exports.

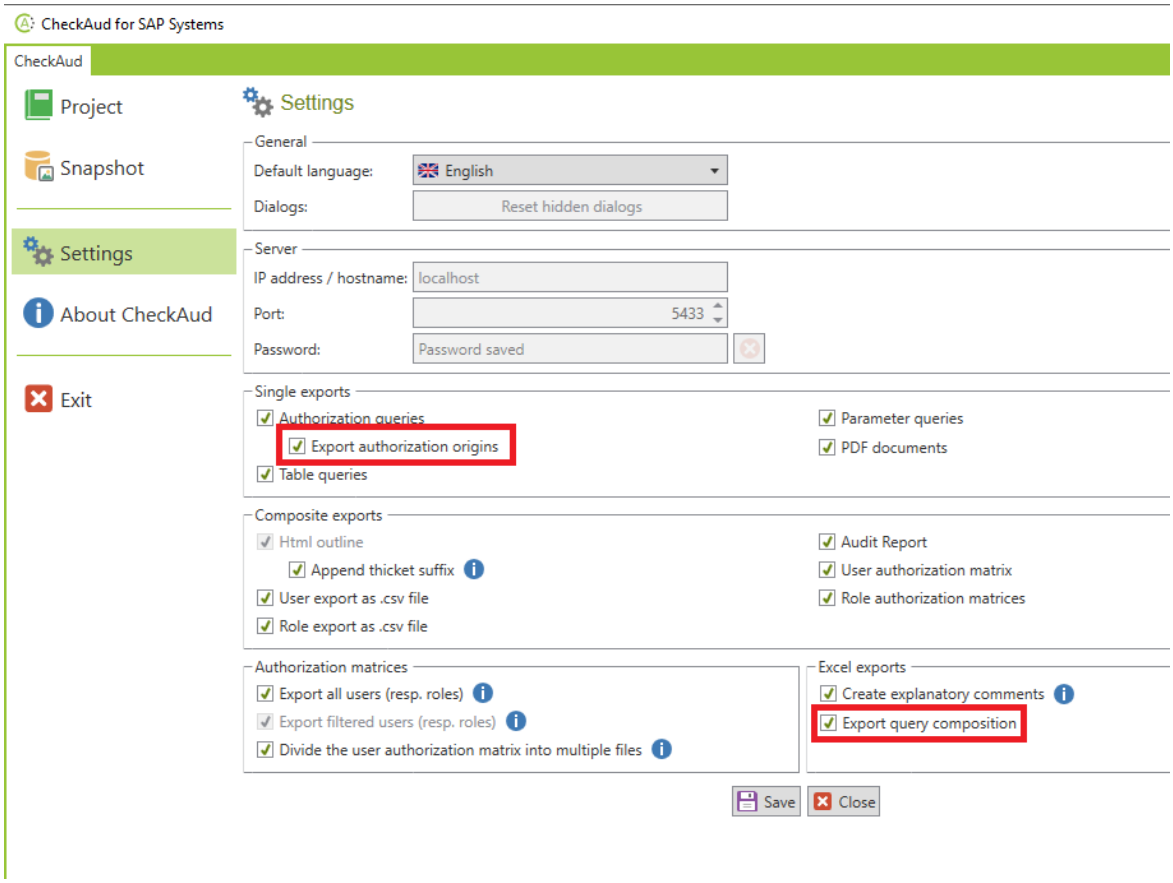



**Figure 213 - Authoriziation origins and Export query composition**

# Chapter IV - Risk management

# IV Risk management

## IV - 1 Introduction

CheckAud is an important component of risk management. It provides a unique perspective on the results of authorization checks and is an efficient solution for assessing system security. As well as technical authorization assignments, you can also include organization-specific characteristics such as technical and organizational exception rules in your assessments. CheckAud uses this information to calculate scores for all your queries, which can then be submitted to your management team in graphical form, for instance. These scores let you document the function and effectiveness of your risk management system, create targeted reports and notifications (event-driven reporting) or highlight improvements or impairments to system security in authorization projects.

## IV - 2 Definition – What is a risk?

Company decisions are made with risk management in mind, and actions are taken with due consideration of their potential positive or negative effects. Companies take prevailing conditions into account as precisely as possible in order to safeguard these decisions and actions and minimize negative effects to the greatest extent possible. In such cases, risk is measured based on its likelihood of occurring and, if it does occur, its potential damage. These estimates form the basis for the use of CheckAud within the context of risk management.

## IV - 3 Configuring risk management

### IV - 3.1 Description and documentation of risks

The basis for the risk management system is the technical description of the risk related to the query selected. IBS supplies predefined risk descriptions (in German or English) for its standard queries. These descriptions can be used and adapted to company-specific characteristics where necessary. Documentation is used to provide a detailed description of the risk, and includes keywords and recommendations for defining actions

### IV - 3.1.1 Risk description & documentation for the authorization query

To open the risk description for an authorization query, you must select the authorization query in the analysis project. The risk description and other related settings can be found on the *Risk Management* tab page in the main window.

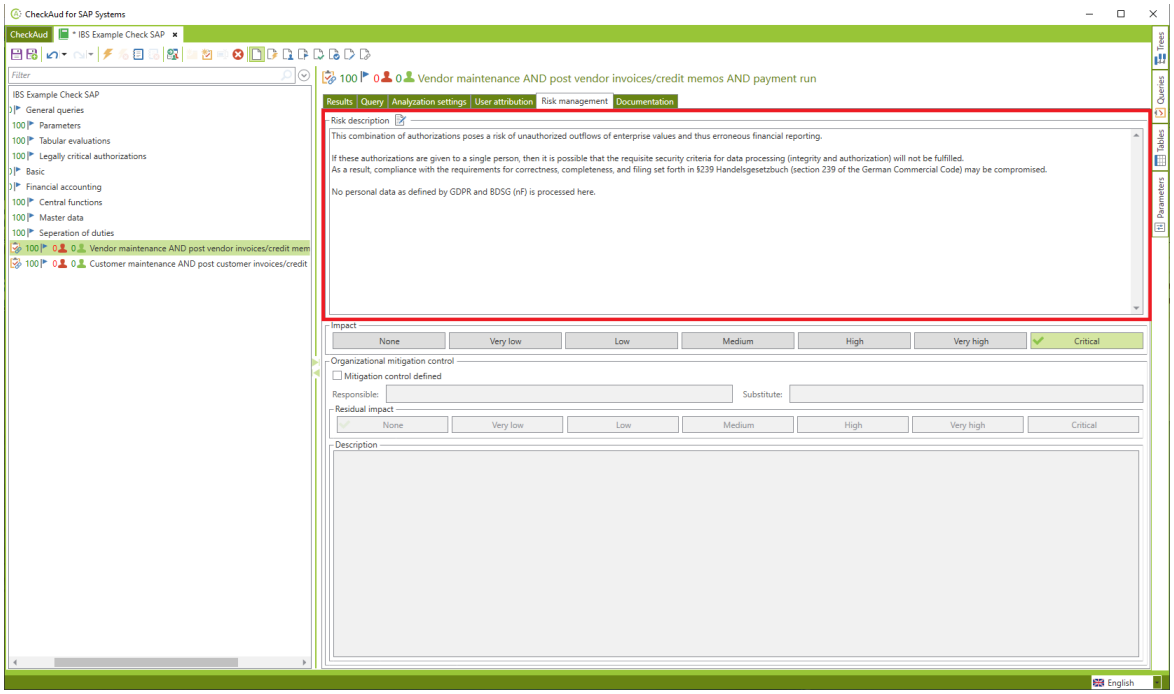



**Figure 214 - Risk description**

On the *Documentation* tab, you can enter additional information for each authorization query in CheckAud and use it to better classify the priority of the query for risk management.


**Figure 215 - Documentation and recommended actions**

*Tags*
You can enter keywords separated by commas in this free text field. This enables searches within the analysis project or in the overview of all the authorization queries in CheckAud 2025.2. The tags can be entered in German and English, if you switch the language using the language selection.

You enter one or several keywords and various key terms and the relevant queries that contain these terms are displayed in a list.

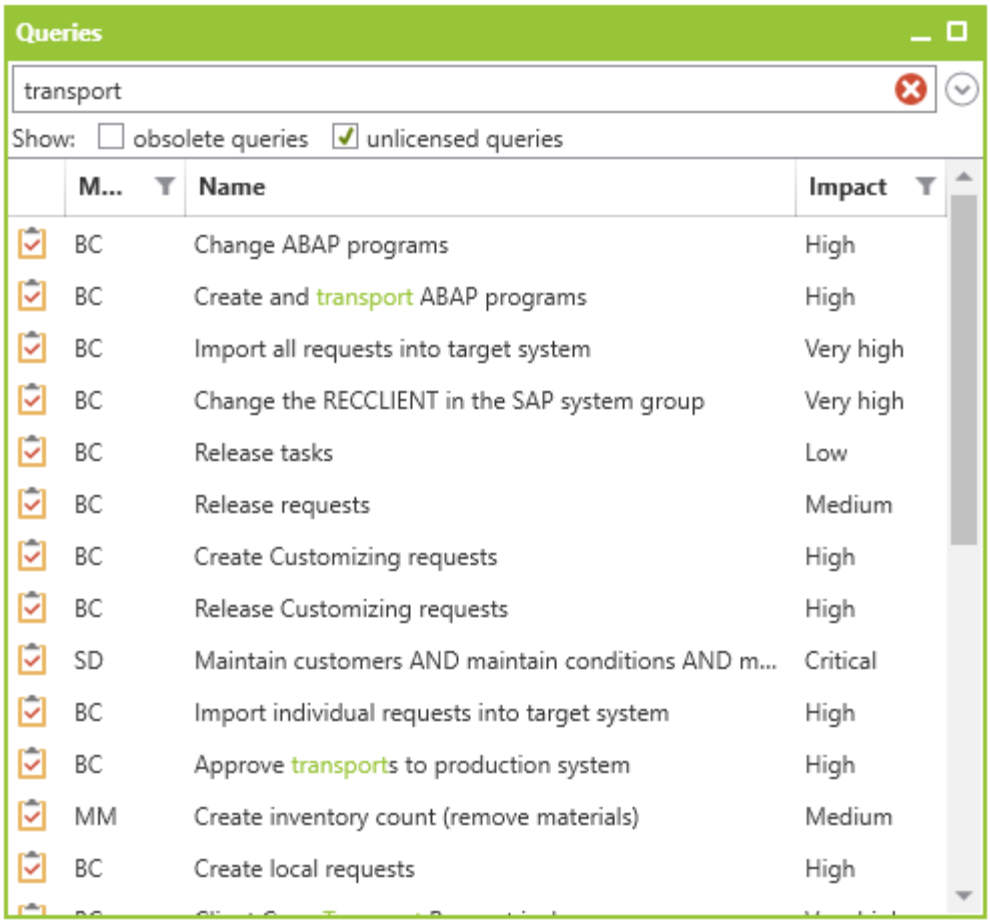



**Figure 216 - Search using keywords**

*Scope*
In this free text field, you can describe the intended scope of this query. This helps you to better organize and assess the query. The information can be entered in German and English, if you switch the language using the language selection.

*Objectives*
You can define the objective of the query in this free text field. It lets you describe the purpose of the query and the intended goal of the improvements based on the query results in more detail. The information can be entered in German and English, if you switch the language using the language selection.

### IV - 3.1.2 Risk description & documentation for the table query

In contrast to authorization queries, only the documentation can be maintained for table queries:

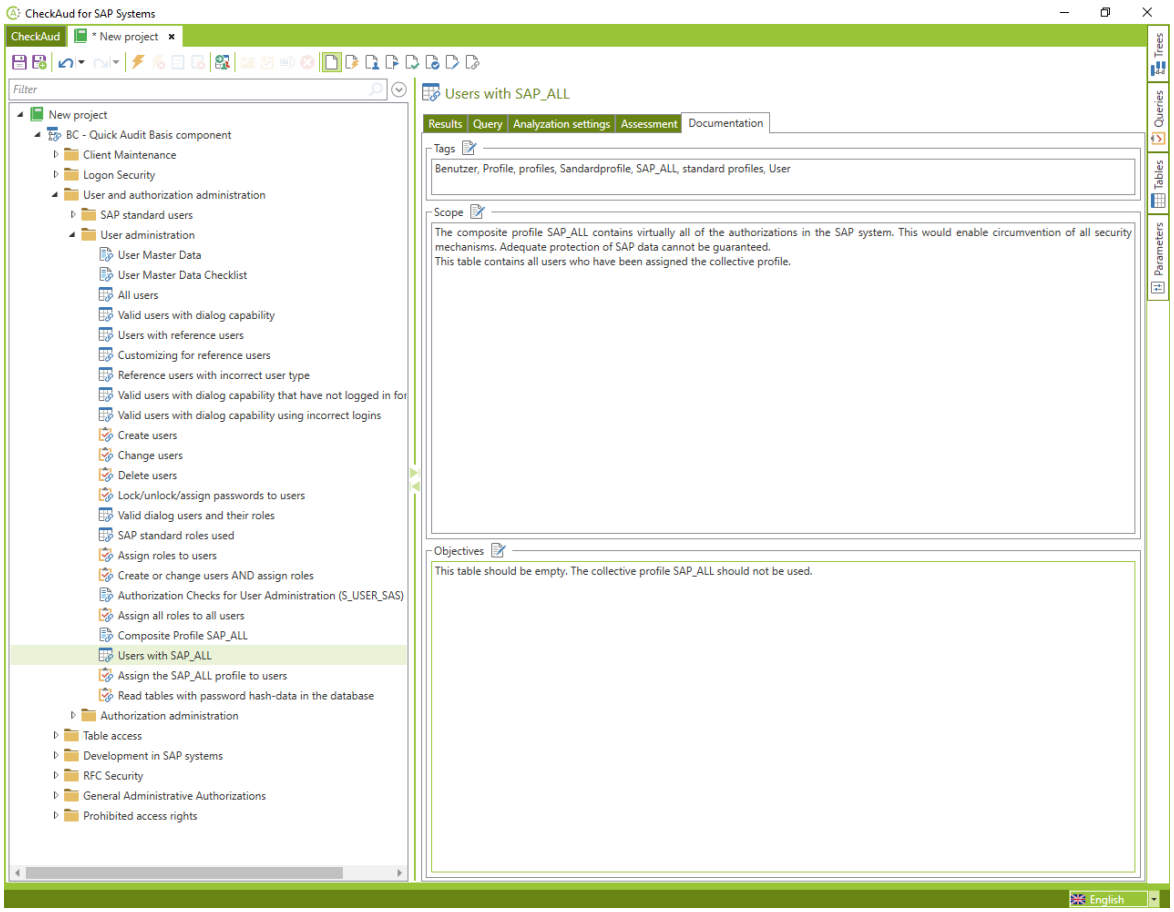



**Figure 217 - Documentation for a table query**

### IV - 3.1.3 Risk description & documentation for the parameter query

In contrast to authorization queries, only the documentation can be maintained for parameter queries:

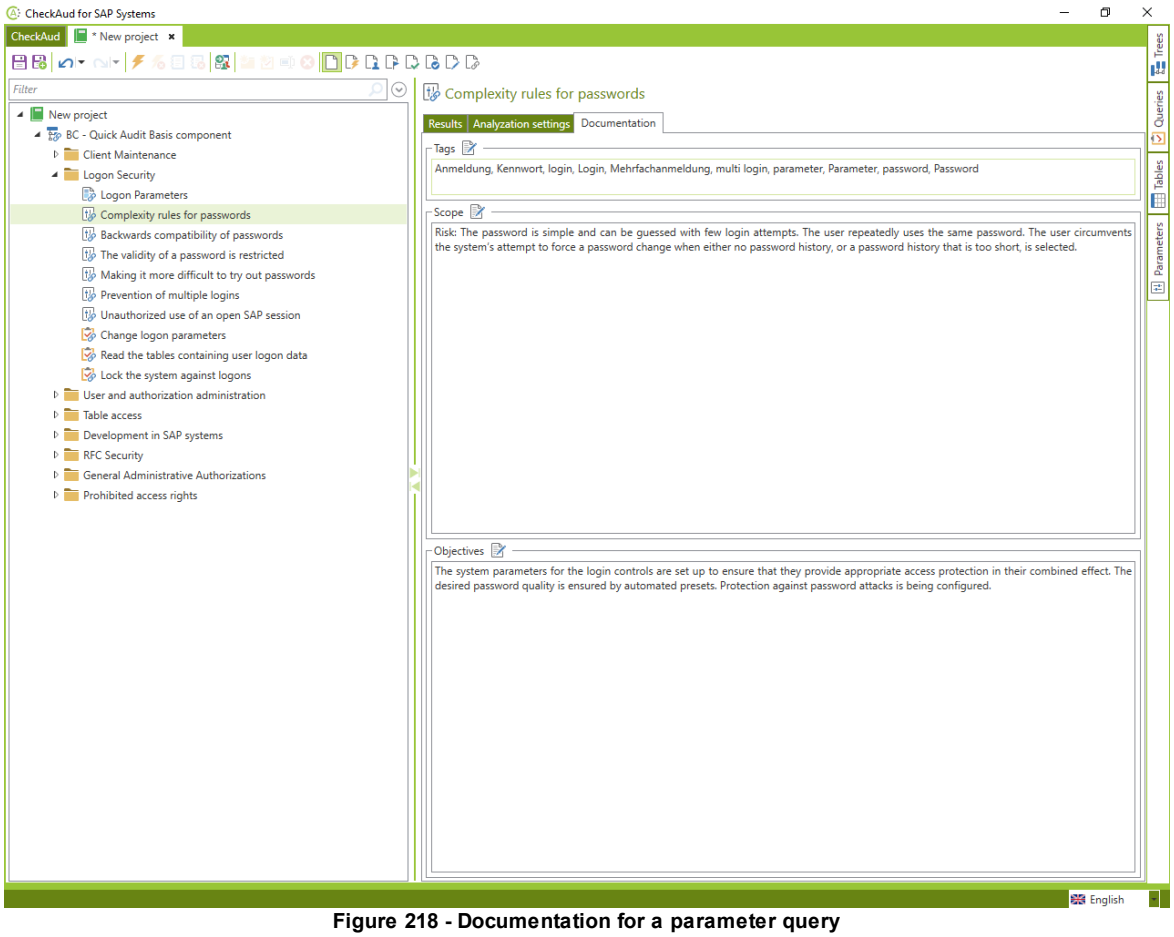



**Figure 218 - Documentation for a parameter query**

### IV - 3.1.4 Changing the risk description and documentation

The free text fields for the risk description and on the *Documentation* tab can be amended if necessary. You can click the  button to edit the relevant free text field.

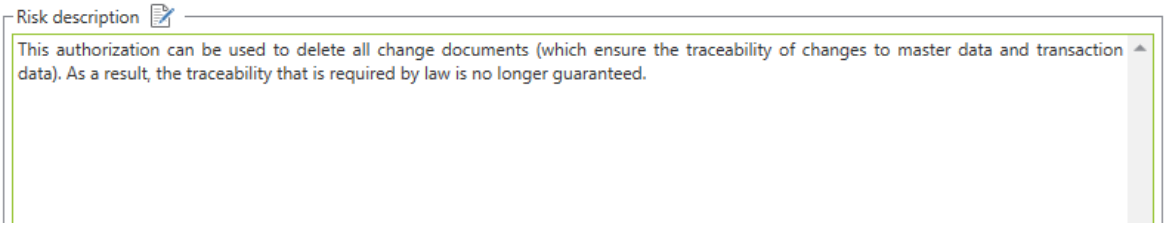



**Figure 219 - Modifying the risk description**

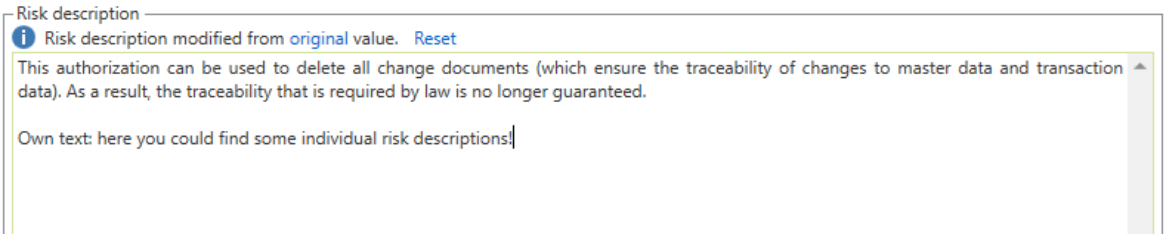



**Figure 220 - Amending the risk description**

The original button displays the original risk description in a separate popup window. The amended risk description remains unchanged. You can use the Reset , button to reset the edited risk description to the default value.

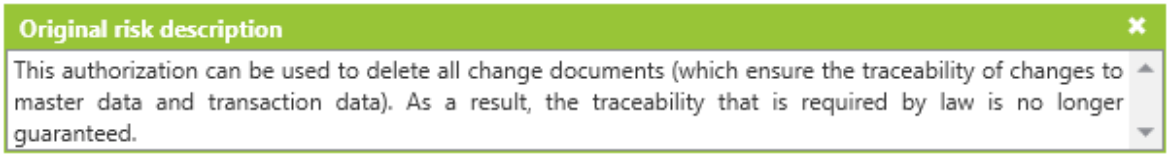



**Figure 221 - Default value of the risk description**

Note that any amendments to the risk description apply only within the current project. The text fields on the *Documentation* tab can be edited using the same procedure described above.

### IV - 3.1.5 Customer documentation

The documentation tab can be extended with tabs for customer's own documentation. This concerns any element in a project, tables, trees, queries, parameters.

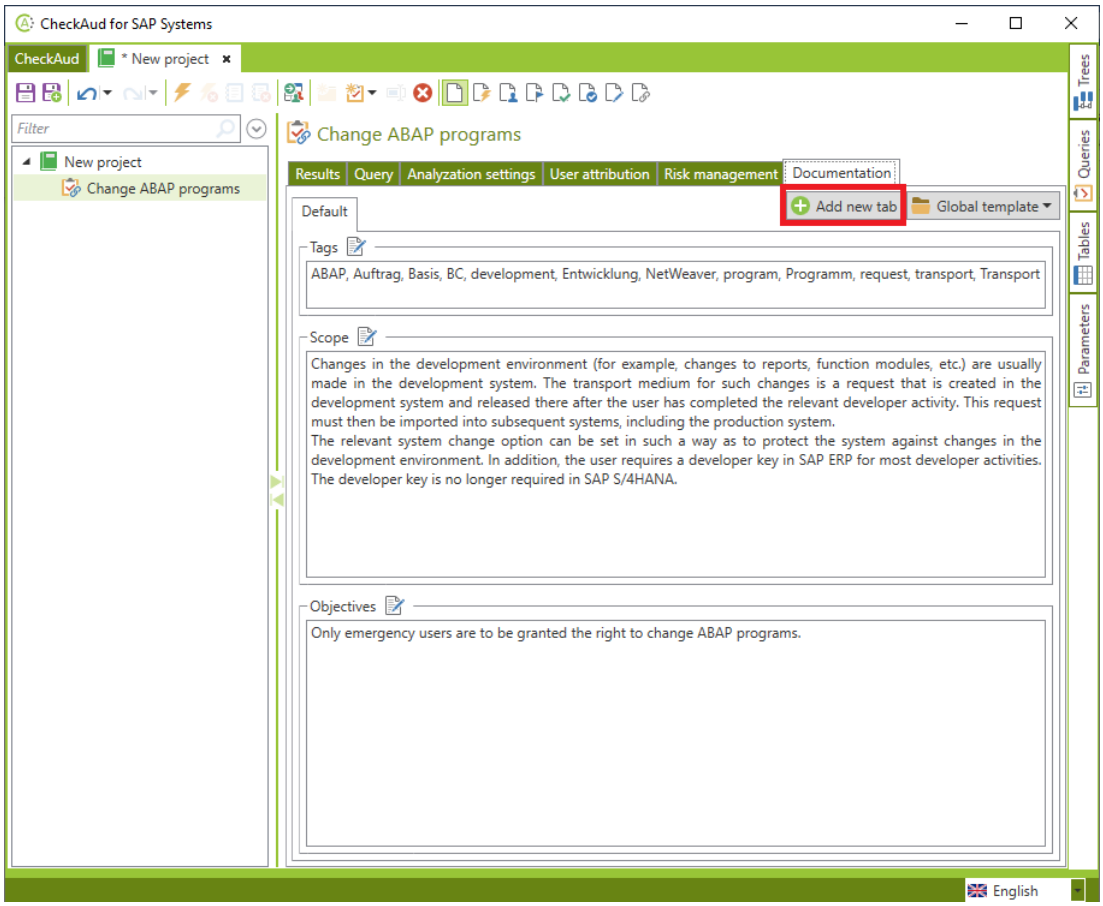



**Figure 222 - Customer documentation**

Via the button "Global template" the documentation setting (the arrangement of tabs and text fields) can be saved and deleted as a template for newly created CheckAud® projects.

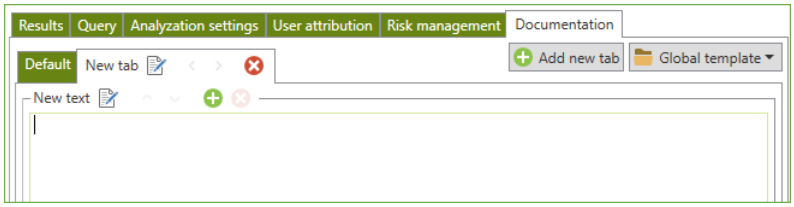



**Figure 223 - Set up Global Template**

## IV - 3.2 Effect of the risk

### IV - 3.2.1 Effect of the risk - authorization queries

The effect describes the level of damage if the risk occurs. This estimate is based on the experiences of the company and must therefore be individually defined. Appropriate estimates of damage are preset for the IBS standard queries and can be individually changed if necessary.


**Figure 224 - Default value for the risk description**

These settings influence the calculated score. More detailed information can be found in the chapter *The Analysis Project Score*.

You can also document a compensating control in CheckAud in addition to the effect of the authorization query risk. If it is not possible to technically safeguard a critical process using authorization assignments in the SAP system, you can configure a non-technical control.

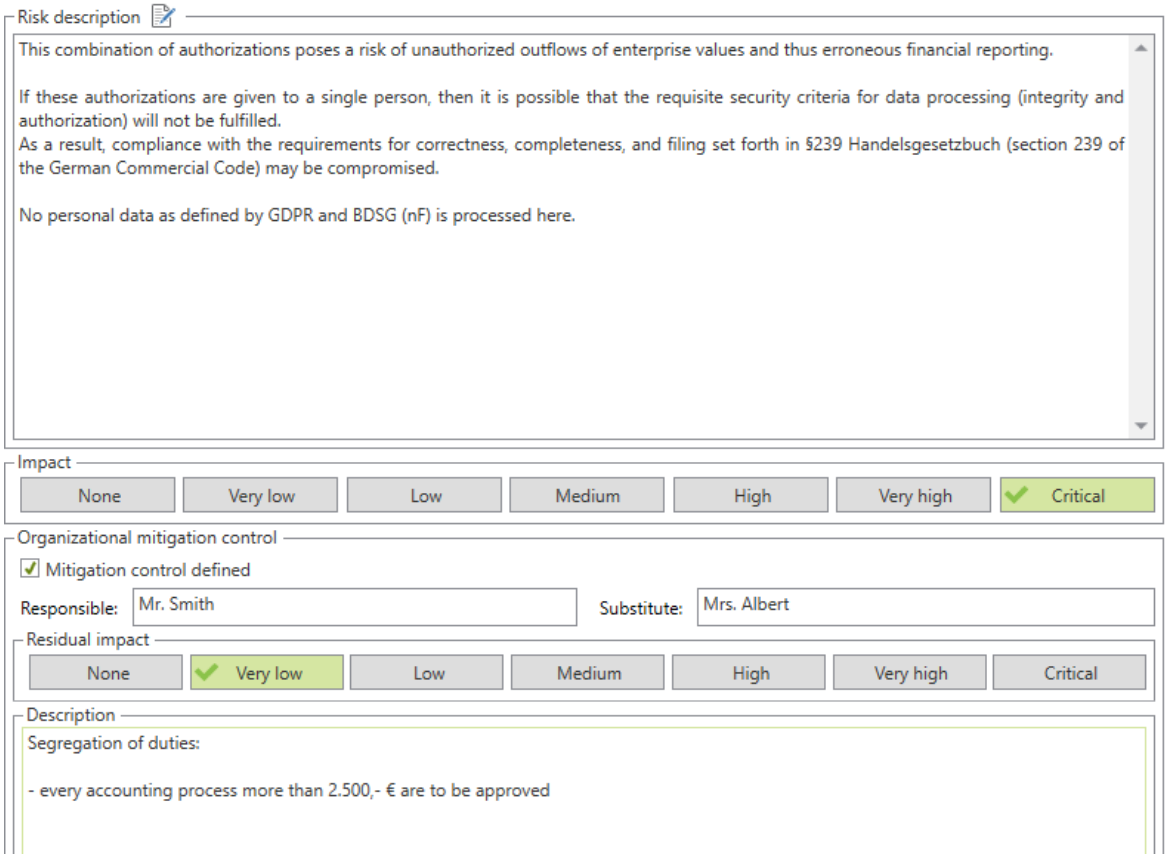



**Figure 225 - Documentation for a compensating control**

You can individually define the effect of a risk in the usual way. Use the *Mitigation control defined* flag to activate the *Residual impact* setting. The compensating control is intended to compensate for the actual damaging effect through the definition of an organizational action. Therefore, the *Residual impact* defined must be lower than the initial effect without the compensating control. A technical description including a rule with regard to responsibilities helps to document this non-technical control measure. The definition of this compensating control and the reduced damage

effect associated with it improves the score calculated for this authorization query. More detailed information can be found in the chapter *The Analysis Project Score*.

### IV - 3.2.2 Effect of the risk - table queries

Effects of risk are not maintained for table queries.

### IV - 3.2.3 Effect of the risk - parameter queries

The effects of risk are also maintained through the usual steps for system parameters. If the parameter queries are based on the queries delivered as standard by IBS Schreiber GmbH, the effects are predefined and cannot be changed.

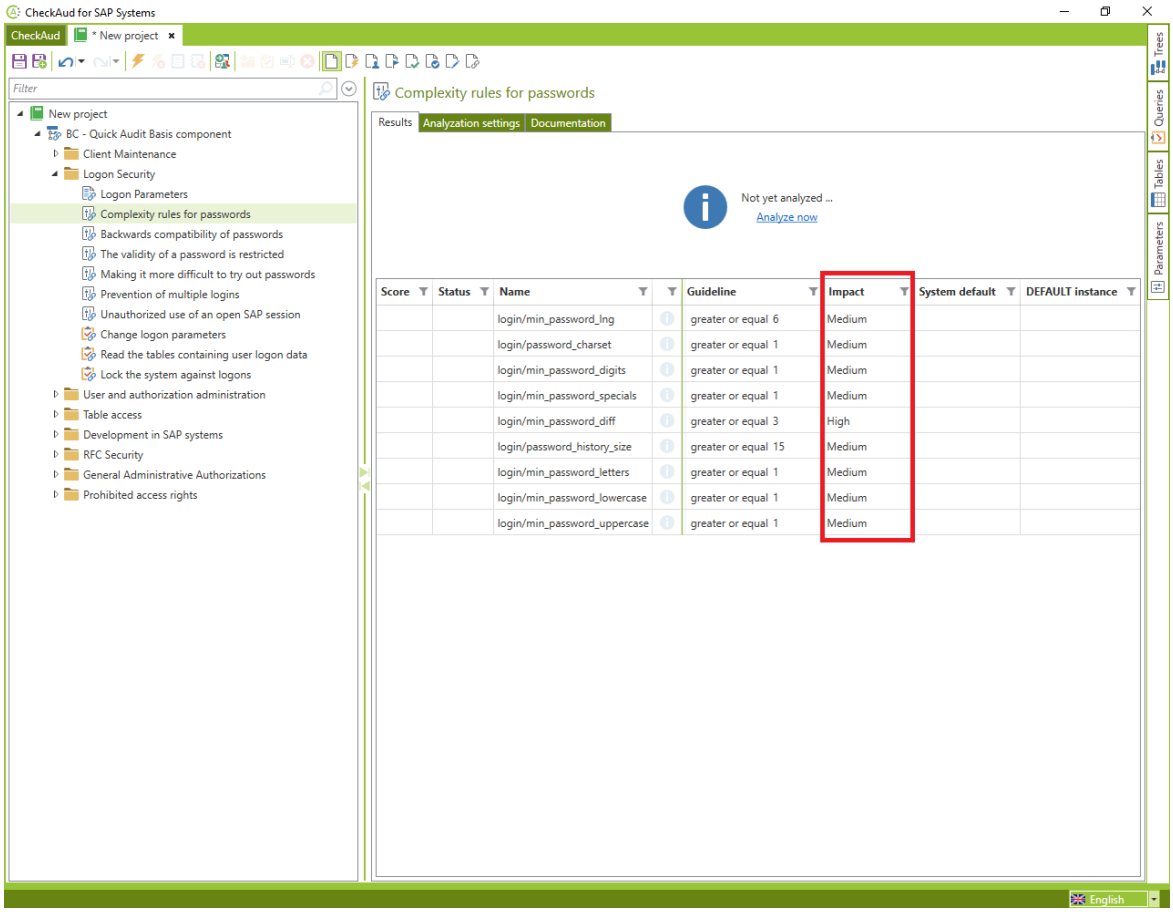



**Figure 226 - Effect of risk in parameter queries**

You can configure the effect of risks for queries that you define yourself. For more information, see the chapter *Adapting the Analysis Project*.

## IV - 3.3 User attribution in authorization queries

You can use the user assignment to define exception rules (target specifications) for the authorization queries. Users with high-level authorizations (technical users, user users) that should not be used for the risk assessment are often included in the results. In addition, there are users that are legitimate for a queried authorization based on the organizational structure. These users

must also be excluded from the risk assessment, because they require the authorization to fulfill their tasks. With that in mind, you can define rules that can be used to identify users as legitimate for the query. The differentiated definition of users has a direct influence on the calculation of the score.

Click Add criterion to add a user assignment for the applicable authorization query. If multiple individual criteria are logically combined in one criteria block, you can create them one after the other using the button. Individual criteria can be linked with a logical OR and/or AND. Multiple criteria blocks are always created as OR links.

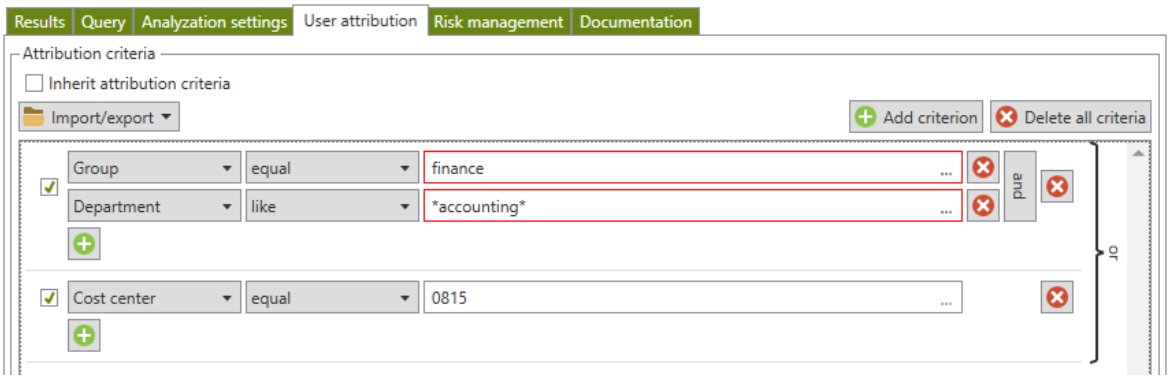



**Figure 227 - User attribution**

You can use the following SAP user account attributes for the rules:
- User (user ID)
- Type
- Lock
- Valid from
- Valid to
- Group
- Department
- Role
- Cost center
- User Groups

You can use the following HANA DB user account attributes for the rules:
- User
- Valid from
- Valid to
- Restricted
- Deactivated
- User group

The attributes can be selected with the following relational operators, depending on the attribute:
- Equal
- Not equal to
- Like
- Unlike
- Includes (enthält)
- Does not include (enthält nicht)
- Less than

- Greater than
- Less than or equal to
- Greater than or equal to

You can use * as a wildcard for the comparison values *Like* and *Unlike*.

As a basic principle, the rules are inclusion rules; that is, users that fulfill the rule are legitimate for the authorization. Any users that do not fulfill the rule are not legitimate. Rules can be inherited in specific ways within a project.

The example below shows how to legitimize specific users for an authorization query:

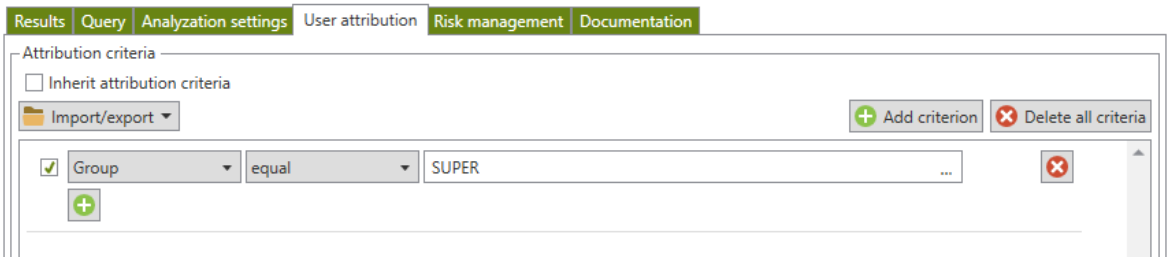



**Figure 228 - All users in the group SUPER are legitimate for the authorization query**

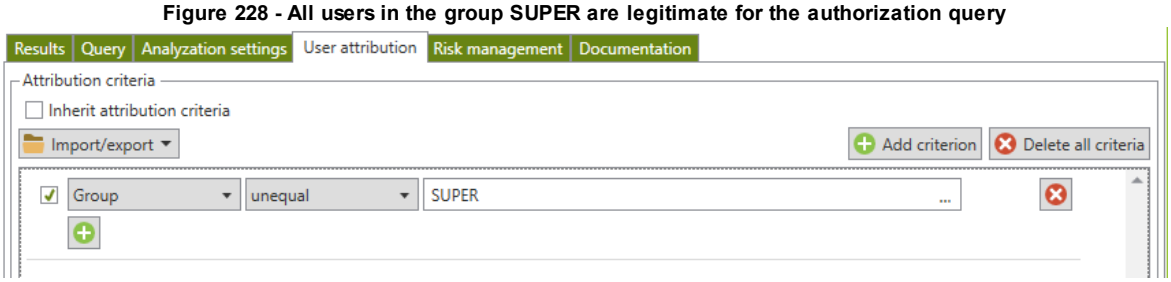
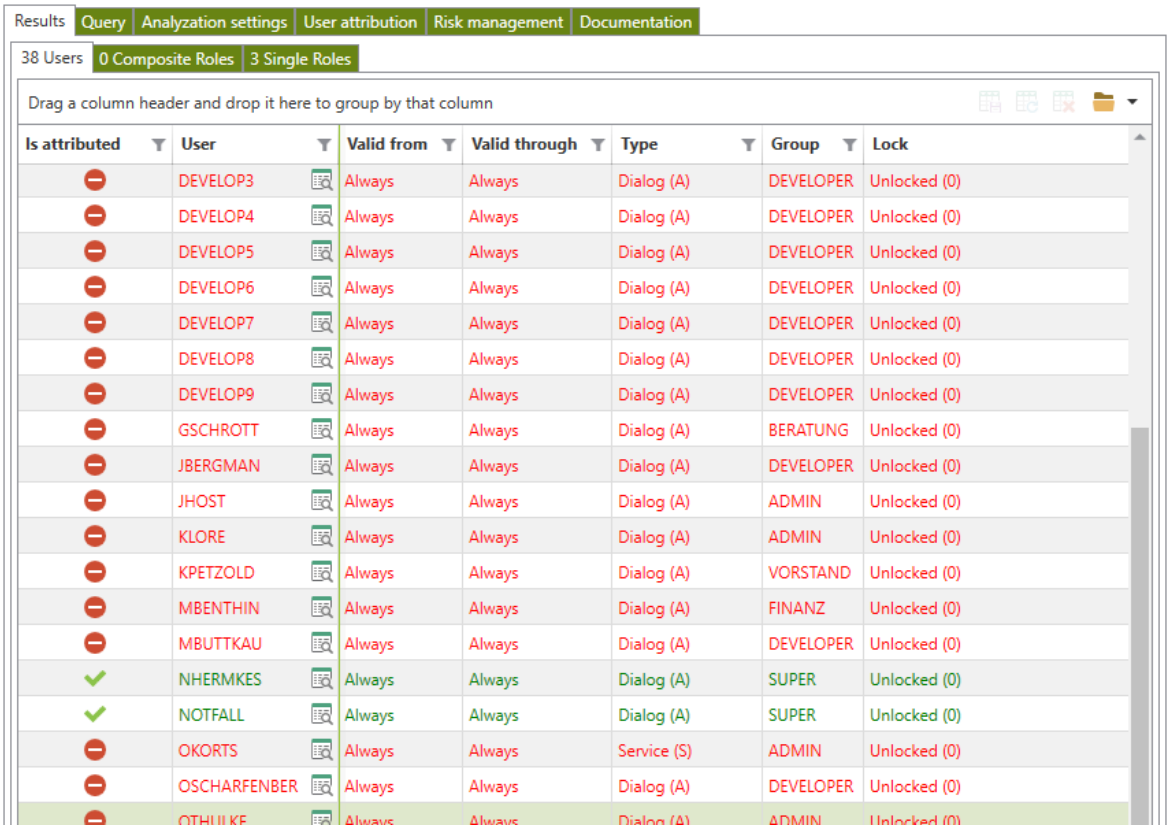



**Figure 229 - All users apart from users in the group SUPER are legitimate for the authorization query**




| Is attributed | User | Valid from | Valid through | Type | Group | Lock |
|---|---|---|---|---|---|---|
| ⛔ | DEVELOP3 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | DEVELOP4 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | DEVELOP5 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | DEVELOP6 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | DEVELOP7 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | DEVELOP8 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | DEVELOP9 | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | GSCHROTT | Always | Always | Dialog (A) | BERATUNG | Unlocked (0) |
| ⛔ | JBERGMAN | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | JHOST | Always | Always | Dialog (A) | ADMIN | Unlocked (0) |
| ⛔ | KLORE | Always | Always | Dialog (A) | ADMIN | Unlocked (0) |
| ⛔ | KPETZOLD | Always | Always | Dialog (A) | VORSTAND | Unlocked (0) |
| ⛔ | MBENTHIN | Always | Always | Dialog (A) | FINANZ | Unlocked (0) |
| ⛔ | MBUTTKAU | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ✓ | NHERMKES | Always | Always | Dialog (A) | SUPER | Unlocked (0) |
| ✓ | NOTFALL | Always | Always | Dialog (A) | SUPER | Unlocked (0) |
| ⛔ | OKORTS | Always | Always | Service (S) | ADMIN | Unlocked (0) |
| ⛔ | OSCHARFENBER | Always | Always | Dialog (A) | DEVELOPER | Unlocked (0) |
| ⛔ | OTHULKE | Always | Always | Dialog (A) | ADMIN | Unlocked (0) |

**Figure 230 - Results display with user assignment**

**Note:** A newly created user assignment is activated only once the authorization query is evaluated again.

You can use the 

button to load or save user assignments. An import of user attributions from a TXT file will also be available for selection. The TXT file may contain only one user ID per line:

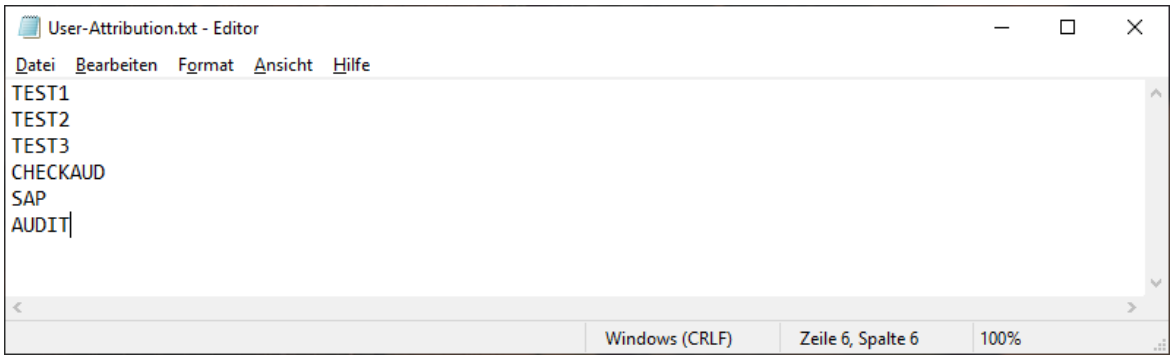



**Figure 231 - Importing a TXT file for a user assignment**

You can use the 

button to open a dialog window for selecting predefined user assignments. Here, the file format must be changed from *.causeattribution to *.txt:

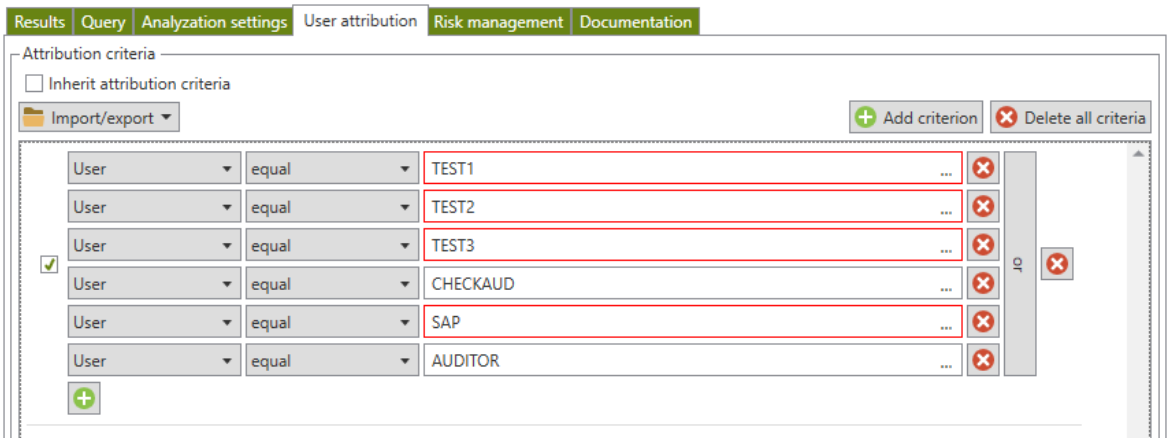



**Figure 232 - User assignment based on an imported TXT file**

**Note:** A line surrounded by a red box indicates that the value entered (in this case, for the user name) is not included in the snapshot of the analysis project.

## IV - 3.4 Import user attribution via user-authorization-matrix

For a precise analysis of assigned authorizations, it is sometimes necessary, to define users which are allowed to have access to critical rights or critical combination of rights. Such a user attribution can be configured via two possibilities. First one is to assign single users on the *User attribution* tab on each authorization query. This has to be done manual for each user or each authorization query and should only be used in individual cases. Another way is to use mass import functions to set up multiple user assignements on several authorization queries. This could be necessary during first implementations of CheckAud or due to organizational changes in the company or in the internal processes. This import function can be found in the menu bar or via context menu in an analysis project.

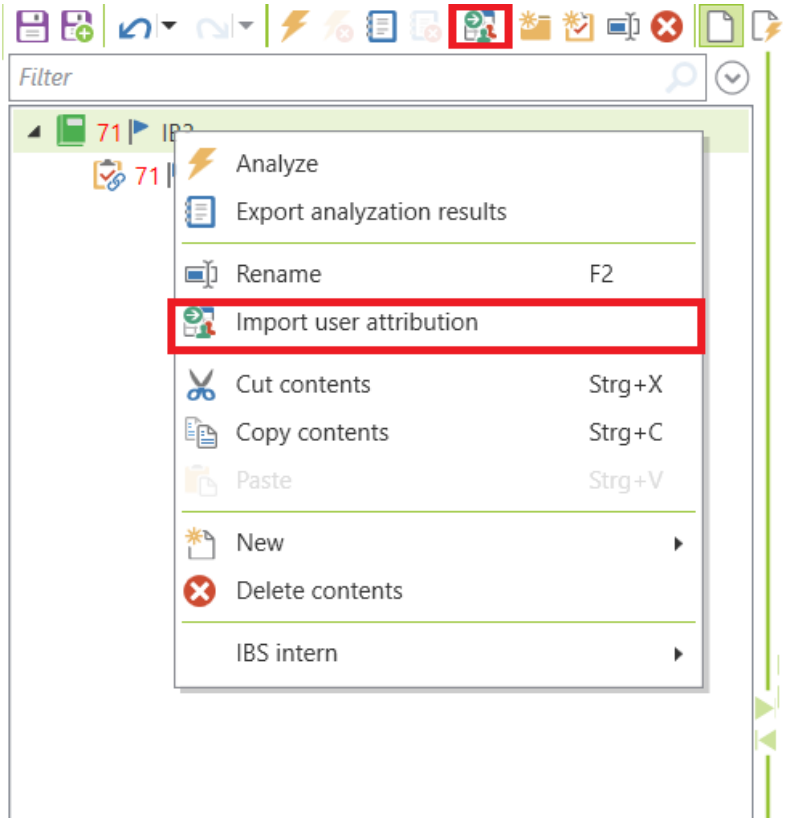


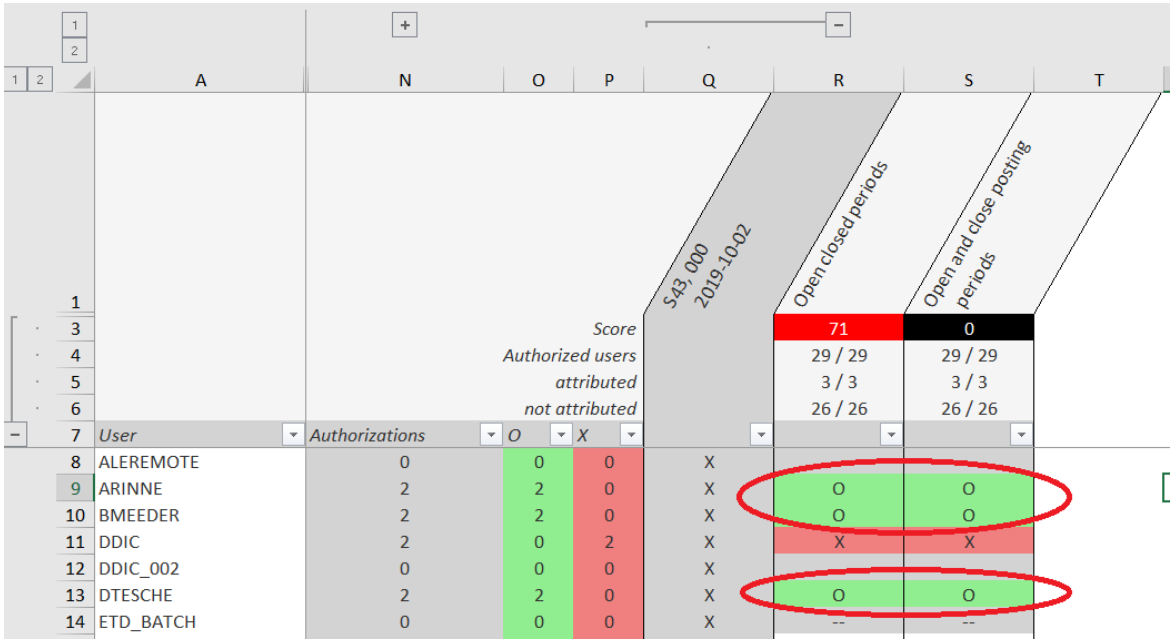

**Figure 233 - start import**

The mass import is based on the user-authorization-matrix which can be generated as a result report of an analysis project:

| | A | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | 543, 000 2019-10-02 | Open closed periods | Open and close posting periods | |
| 3 | | | | Score | | 71 | 0 | |
| 4 | | | | Authorized users | | 29 / 29 | 29 / 29 | |
| 5 | | | | attributed | | 0 / 0 | 0 / 0 | |
| 6 | | | | not attributed | | 29 / 29 | 29 / 29 | |
| 7 | User | Authorizations | O | X | | | | |
| 8 | ALEREMOTE | 0 | 0 | 0 | X | -- | -- | |
| 9 | ARINNE | 2 | 0 | 2 | X | X | X | |
| 10 | BMEEDER | 2 | 0 | 2 | X | X | X | |
| 11 | DDIC | 2 | 0 | 2 | X | X | X | |
| 12 | DDIC_002 | 0 | 0 | 0 | X | -- | -- | |
| 13 | DTESCHE | 2 | 0 | 2 | X | X | X | |
| 14 | ETD_BATCH | 0 | 0 | 0 | X | -- | -- | |

**Figure 234 - Original Benutzer-Berechtigungs-Matrix**

The new assignment can be done by changing the field values of the matrix from "X" to "O". Thus, users are now defined as legitimate for the authorization.



| | A | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|
| | | | | | 543, 000 2019-10-02 | Open closed periods | Open and close posting periods | |
| 3 | | | Score | | | 71 | 0 | |
| 4 | | | Authorized users | | | 29 / 29 | 29 / 29 | |
| 5 | | | attributed | | | 3 / 3 | 3 / 3 | |
| 6 | | | not attributed | | | 26 / 26 | 26 / 26 | |
| 7 | User | Authorizations | O | X | | | | |
| 8 | ALEREMOTE | 0 | 0 | 0 | X | | | |
| 9 | ARINNE | 2 | 2 | 0 | X | O | O | |
| 10 | BMEEDER | 2 | 2 | 0 | X | O | O | |
| 11 | DDIC | 2 | 0 | 2 | X | X | X | |
| 12 | DDIC_002 | 0 | 0 | 0 | X | | | |
| 13 | DTESCHE | 2 | 2 | 0 | X | O | O | |
| 14 | ETD_BATCH | 0 | 0 | 0 | X | -- | -- | |

**Figure 235 - Configured user-authorization-matrix**

The next step is to import the prepared user-authorization-matrix in CheckAud. During this step, each authorization query will set up with the new user attribution.

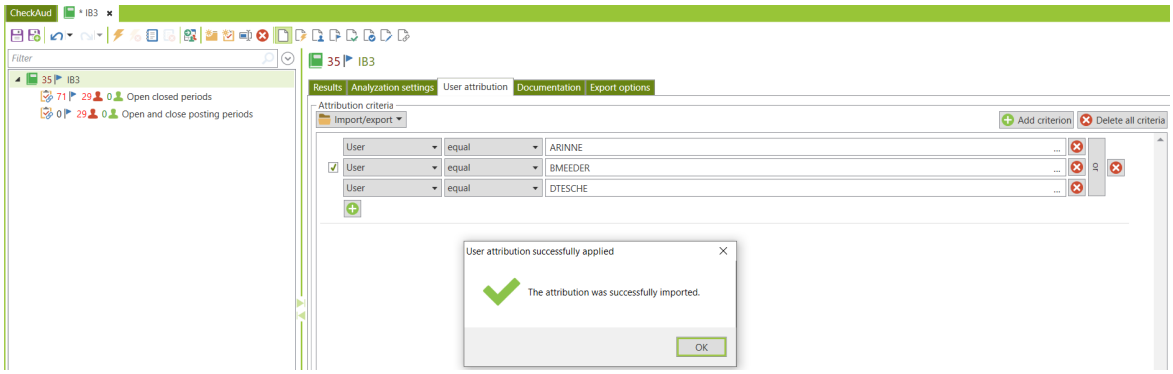



**Figure 236 - Due to import, user attribution is set up**

After import and a new evaluation of the analysis project, due to the ne user attribution all legitimated users will be marked with a "green" label.

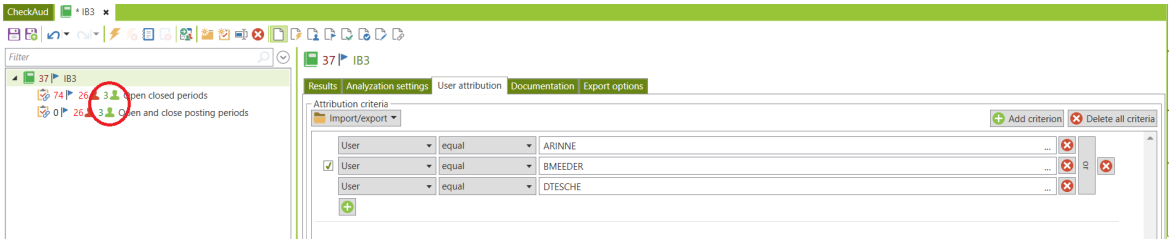



**Figure 237 - Result incl. user attribution**

## IV - 3.5 Inheriting the user attribution

Like the analysis settings, user attributions can also be inherited by subelements within the analysis project. User assignments can be made at project, folder or query level:

Project level: User assignments are inherited to all subelements.

Folder level: User assignments are adopted from the inheritance; alternatively, the inheritance can be interrupted at folder level. In such a case, the new user assignments are inherited to all lower-level elements starting from this level.

Query level: User assignments are adopted from the inheritance; alternatively, the inheritance can be interrupted at query level.In such a case, separate user assignments then apply for these queries.

You can interrupt the inheritance to the individual subelements in general by removing the flag *Inherit attribution criteria*.

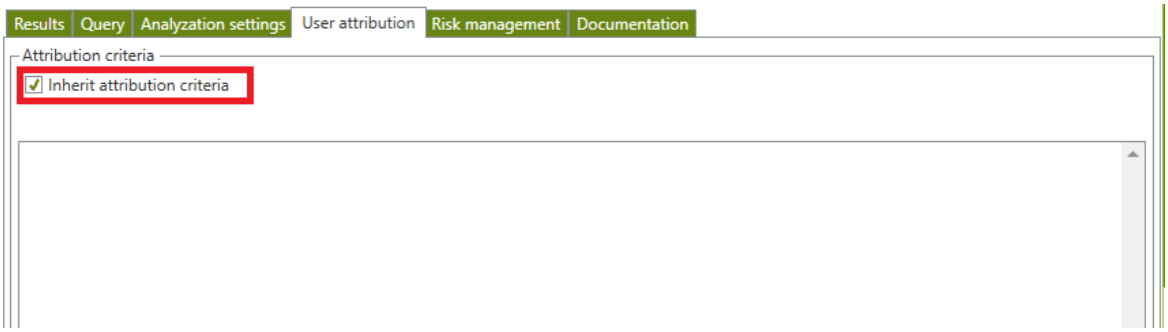



**Figure 238 - Inheriting the user assignment**

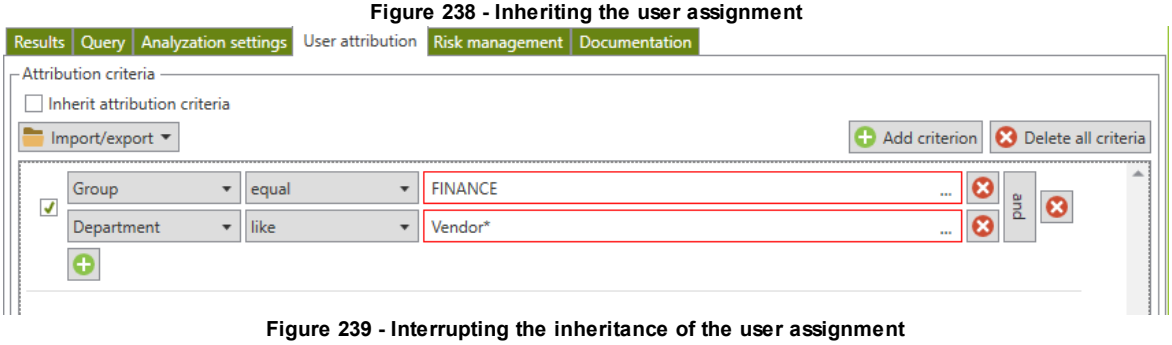



**Figure 239 - Interrupting the inheritance of the user assignment**

To make it easy to identify inheritance interruptions in the analysis project, you can change the view in the analysis project. .

Default analysis project view

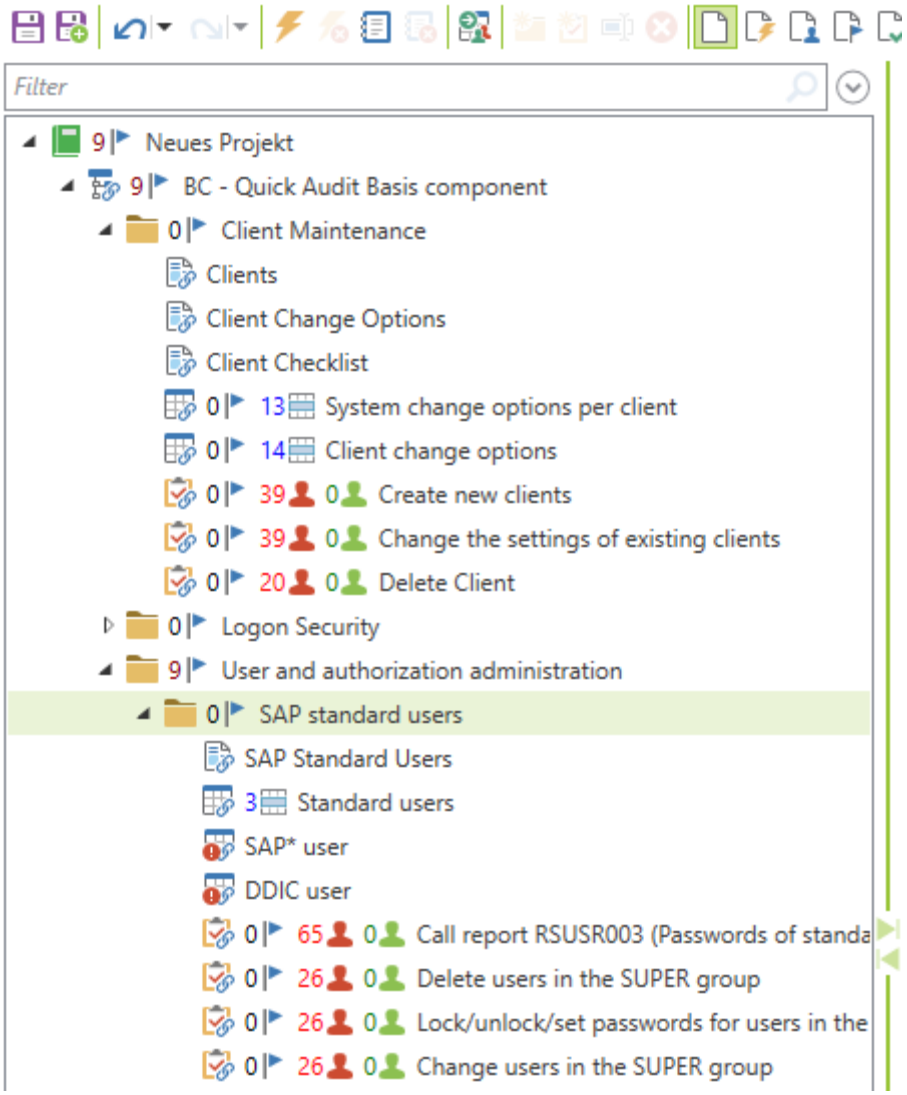



**Figure 240 - Default analysis project view**

Making interruption of transmission in the user assignment known in the tree view of the project

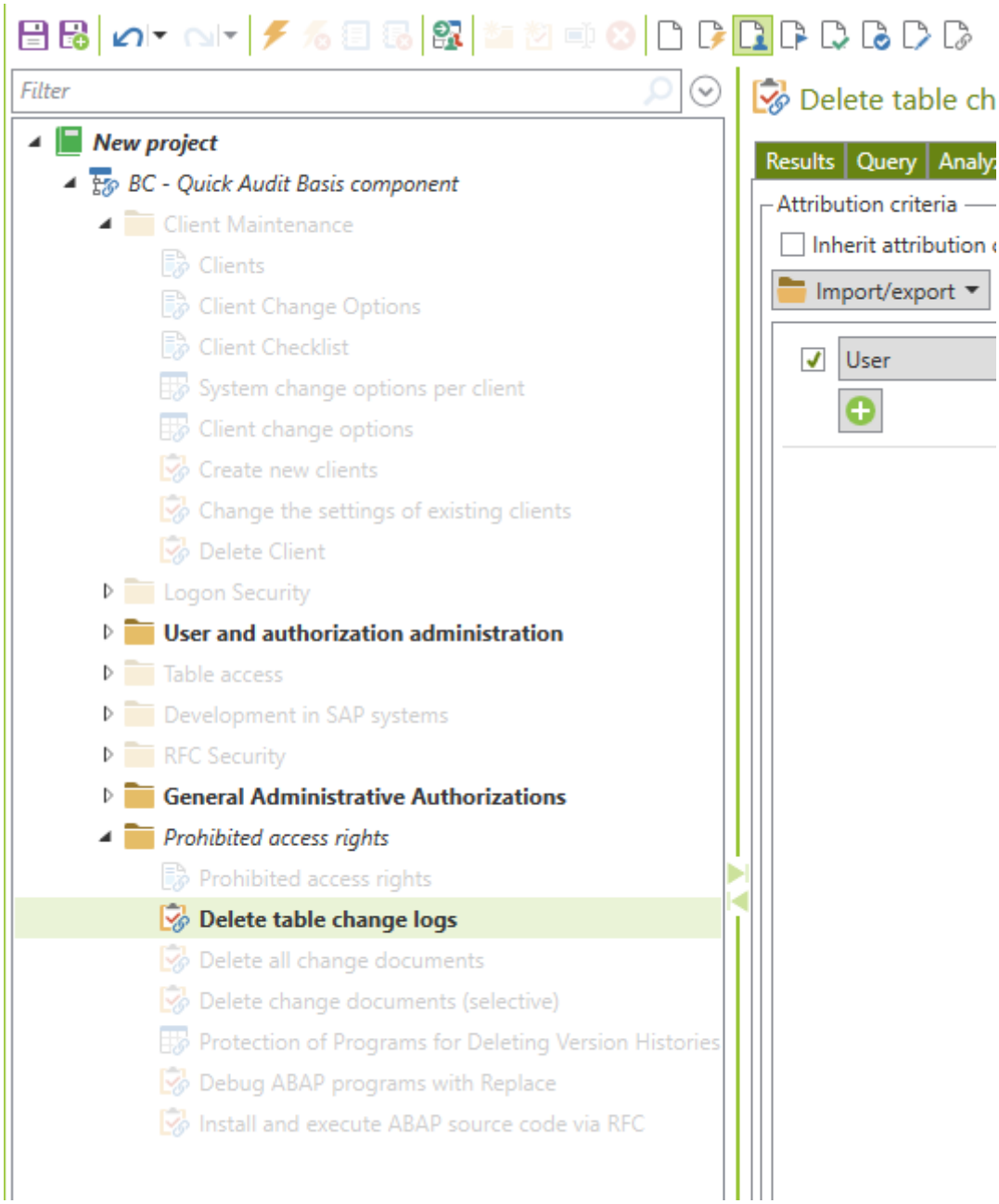



**Figure 241 - Displaying the interrupted inheritance of the user assignment in the analysis project**

If the inheritance of the user assignment is interrupted in individual queries or folders, this can be seen in the tree view with this setting.

## IV - 3.6 Project views for displaying changes in risk management configuration

Any changes in risk description, impact, assessement criterias (on tabular queries) and documentation overriding the standard can be displayed in the analysis project using project views. Relating to the view, the changed queries will be marked in the analysis project.

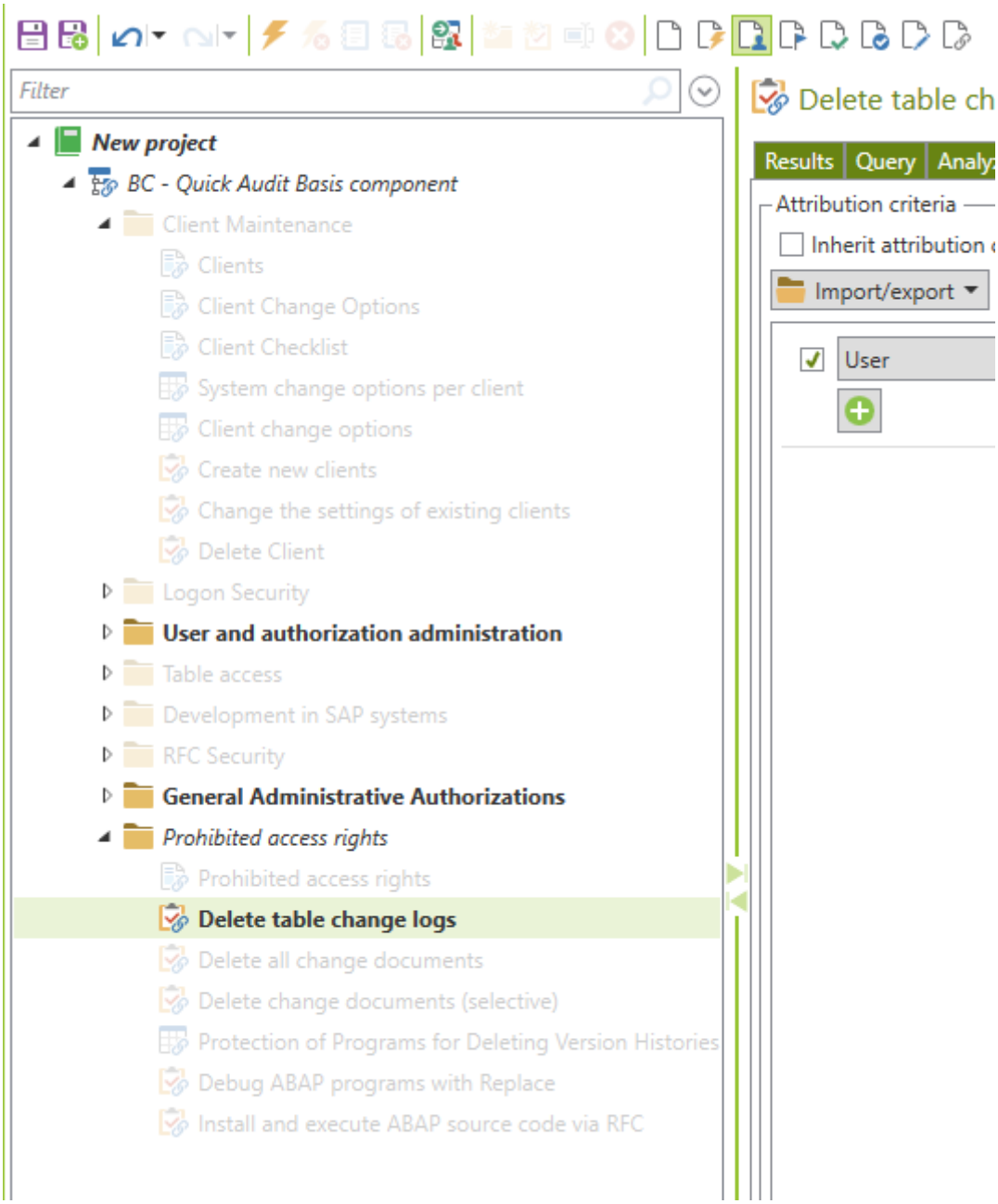



**Figure 242 - visualizing changes in risk management configuration of queries**

For each view there are corresponding buttons in the menu bar:


**Figure 243 - Buttons for project views**

| |
|---|
| visualize changes in impact of authorization queries |
| visualize the definition of mitigation controls of authorization queries |
| visualize changes in assessment criterias of tabular queries |

visualize changes in documentation of authorization queries

## IV - 4 The analysis project score

The analysis project score is a quantitative statement on system security based on the settings for the damage effect, the user assignment and the compensating controls in combination with the results (= authorized found users) for each authorization query, table query and parameter query included in the project. The score is a value between 0 (= low system security, high risk) and 100 (high system security, low risk).

The score is calculated based on the total of all the queries in an analysis project. As part of the process, the individual scores for each directory and/or individual query in the project are determined. Each query can achieve a maximum score of 100. This score is achieved either if the query is not relevant in terms of its effect (the effect is set to None (Keine)) or if the result meets the target specifications, taking all the settings into account.

If deviating results are determined (= authorized but not legitimate users, deviating parameter settings, deviating results in the table queries), a penalty factor is calculated and then deducted from the maximum score of 100. The lowest possible score is 0, so any penalty factor, however high, can never result in a score lower than 0 for a query or project.

The penalty factor is comprised of the following parts:

- Likelihood of occurrence (= the number of technically authorized users in an authorization query)

  The number of users found to be authorized determines the likelihood of occurrence. The more users that are technically authorized, the higher the likelihood that the queried authorization will be used, and the higher the calculated penalty factor as a result.

- User attribution (= exception rules for users found to be authorized in an authorization query)

  If technically authorized users are legitimate users for the queried authorization, these users are not used to assess the likelihood of occurrence. Only users who are technically authorized but not legitimate are used to calculate the penalty factor.

- Effect (= individual priority based on estimated damage)

  The higher the damaging effect, the higher the penalty factor and the greater the reduction in the score if it occurs.

- Compensating control

  If no technical safeguards can be provided in the SAP system, the original damaging effect can be reduced by defining this organizational control. In this case, the reduced effect is included in the calculation of the penalty factor.

The number of users resulting in a score of 0 based on effect are shown below:

| | | |
|---|---|---|
| *Critical* | 1 | Technically authorized but not legitimate users |
| *Very high* | 10 | |
| *High* | 25 | |
| *Medium* | 100 | |
| *Low* | 200 | |

| | | |
|---|---|---|
| *Very low* | 1000 | |
| *None* | Unlimited | |

The cockpit view provides a quick overview of the score calculated for an analysis project, including the respective sub-results of the check areas included in the project. In an analysis project, the cockpit view is displayed when you select the project root or a subdirectory that includes evaluated queries:

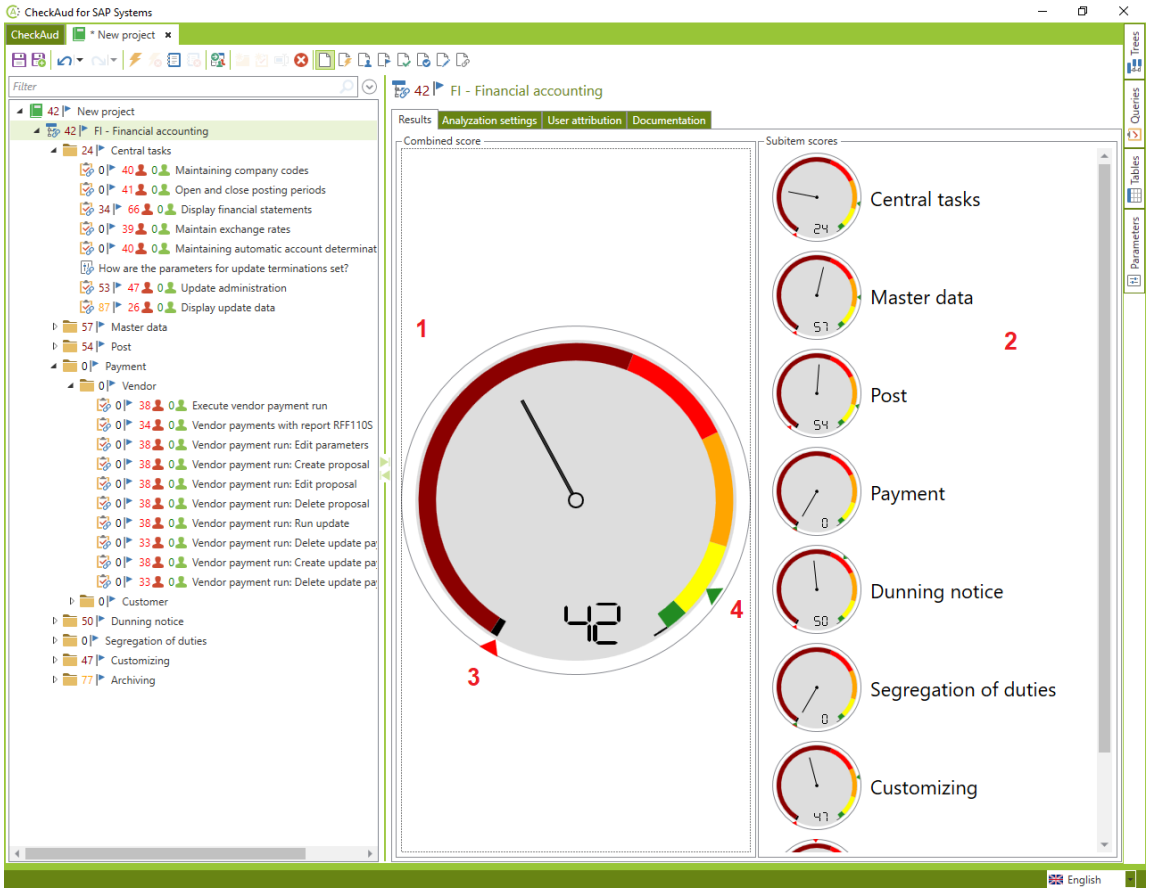



**Figure 244 - Cockpit view**

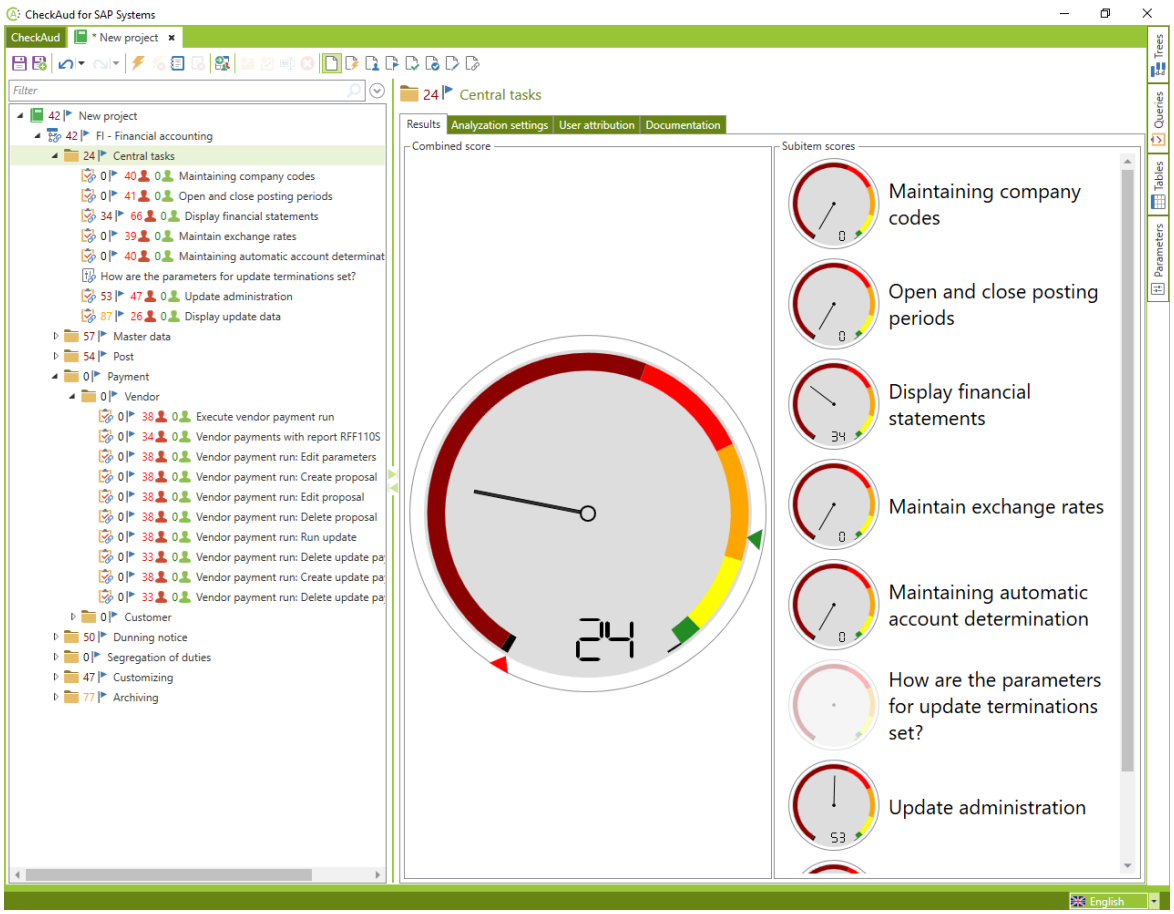
1 Combined score: The score for the element selected in the analysis project, which is calculated based on the respective subelements, is displayed here.

2 Scores of subitems: The respective scores of the direct subitems of the element selected in the analysis project are displayed here.

3 Highest score indicator: Indicates the value range for the maximum score for the analyzed authorization queries.

4 Lowest score indicator: Indicates the value range for the minimum score for the analyzed authorization queries.

You can select elements in the analysis project to create a cockpit view for their subelements:


CheckAud for SAP Systems
CheckAud
* New project
Filter
42 New project
42 FI - Financial accounting
24 Central tasks
0 40 0 Maintaining company codes
0 41 0 Open and close posting periods
34 66 0 Display financial statements
0 39 0 Maintain exchange rates
0 40 0 Maintaining automatic account determinat
How are the parameters for update terminations set?
53 47 0 Update administration
87 26 0 Display update data
57 Master data
54 Post
0 Payment
0 Vendor
0 38 0 Execute vendor payment run
0 34 0 Vendor payments with report RFF110S
0 38 0 Vendor payment run: Edit parameters
0 38 0 Vendor payment run: Create proposal
0 38 0 Vendor payment run: Edit proposal
0 38 0 Vendor payment run: Delete proposal
0 38 0 Vendor payment run: Run update
0 33 0 Vendor payment run: Delete update pa
0 38 0 Vendor payment run: Create update pa
0 33 0 Vendor payment run: Delete update pa
0 Customer
50 Dunning notice
0 Segregation of duties
47 Customizing
77 Archiving
24 Central tasks
Results
Analyzation settings
User attribution
Documentation
Combined score
24
Subitem scores
Maintaining company codes
Open and close posting periods
Display financial statements
Maintain exchange rates
Maintaining automatic account determination
How are the parameters for update terminations set?
Update administration
Trees
Queries
Tables
Parameters
English

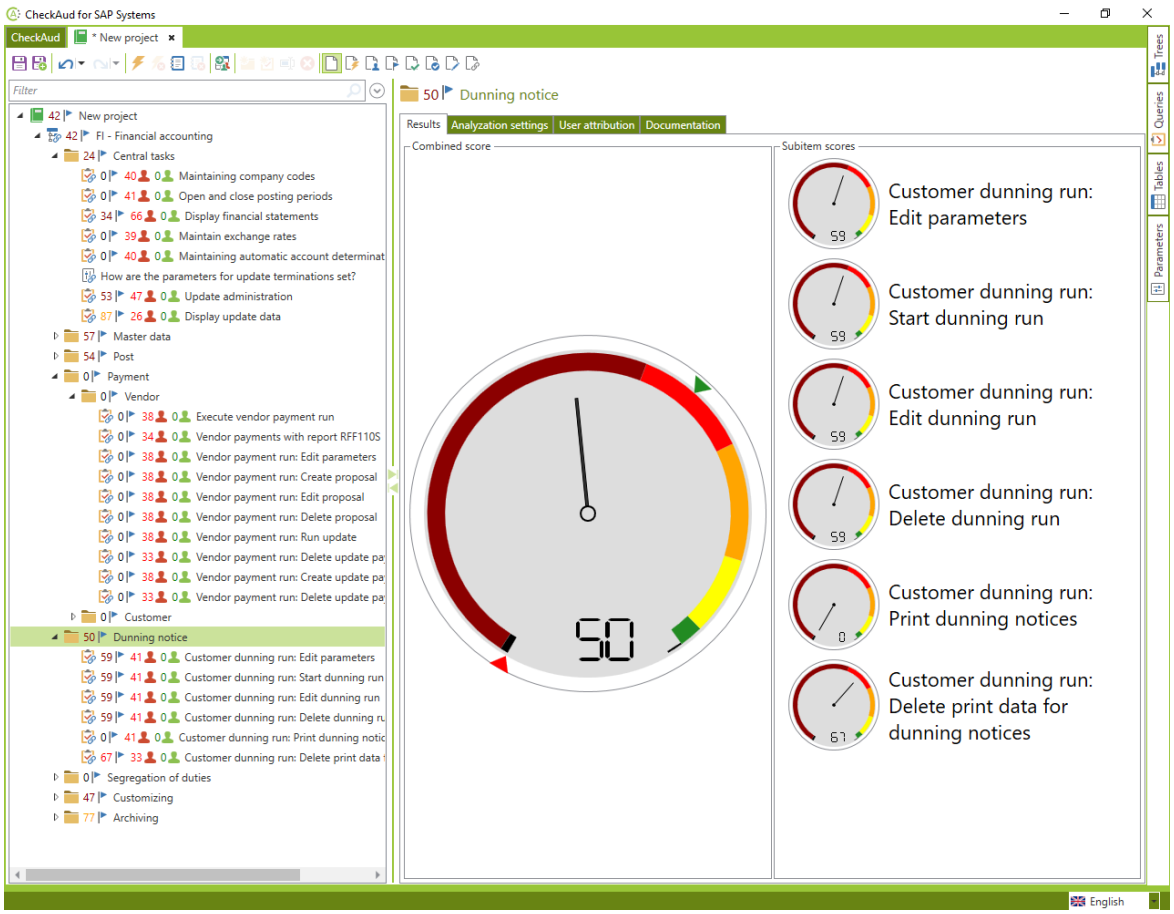



**Figure 245 - Examples of cockpit views**

# Chapter V - Modifying the analysis project

# V Modifying the analysis project

## V - 1 First steps - creating a new project

Click the *New project* button on the *CheckAud* tab page to create a new analysis project. The project view opens:

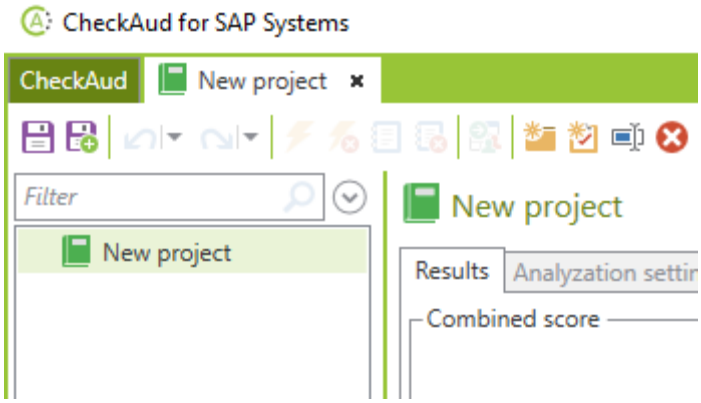



**Figure 246 - New project in the project view**

The following steps must always be performed before additional settings can be configured for the new analysis project:

1. "Filling the empty project with analyses"

   Add a template, individual query, table query or parameter evaluation to the new project using drag and drop.

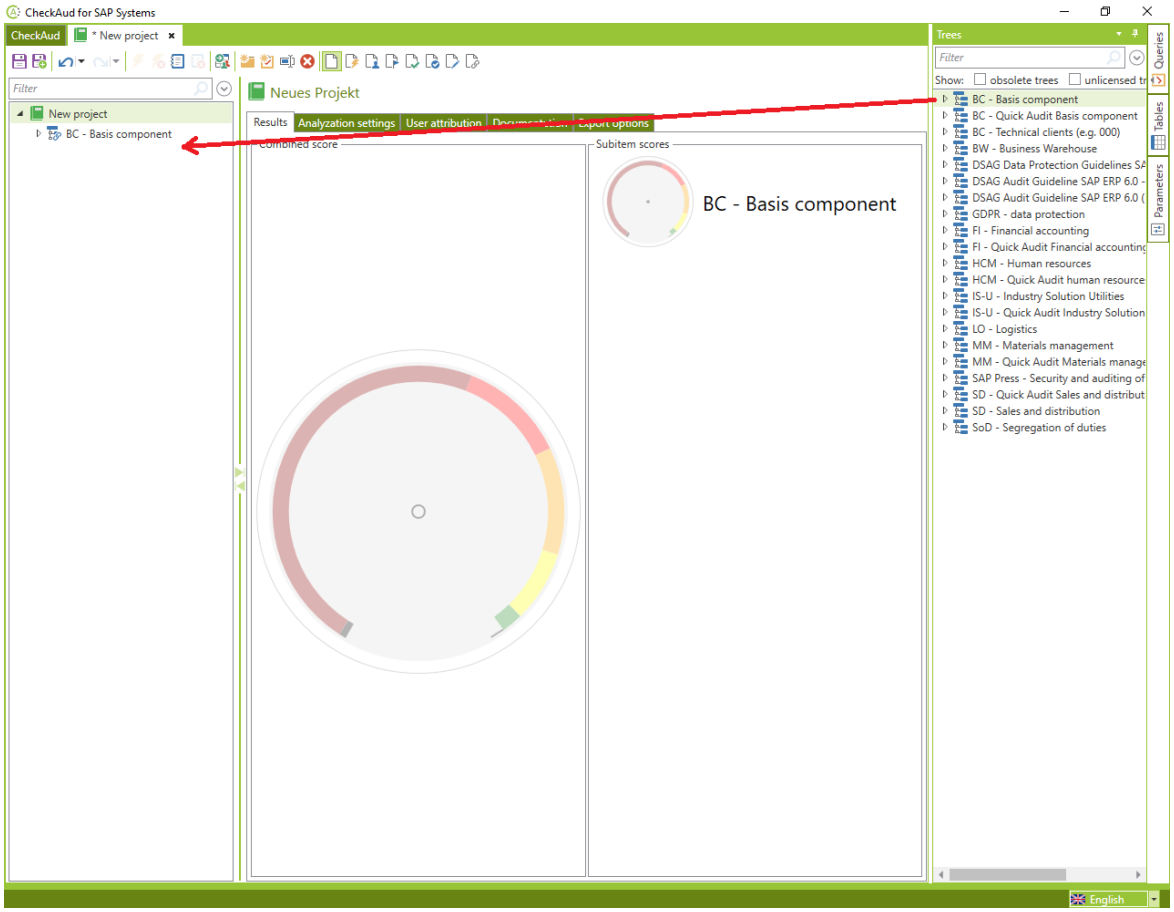



**Figure 247 - Adding project contents using drag and drop**

2. „Filling the project filled with analyses with data“

   Once you have added some project contents, you can select the snapshot you want to use to perform the analysis on the *Analyzation settings* tab page. Attention: when using ABAP and HANA DB queries in the analysis project, there has to be selected a snapshot for an ABAP as well as for a HANA DB system. This can be done using the tabs *ABAP* and *HANA DB*.

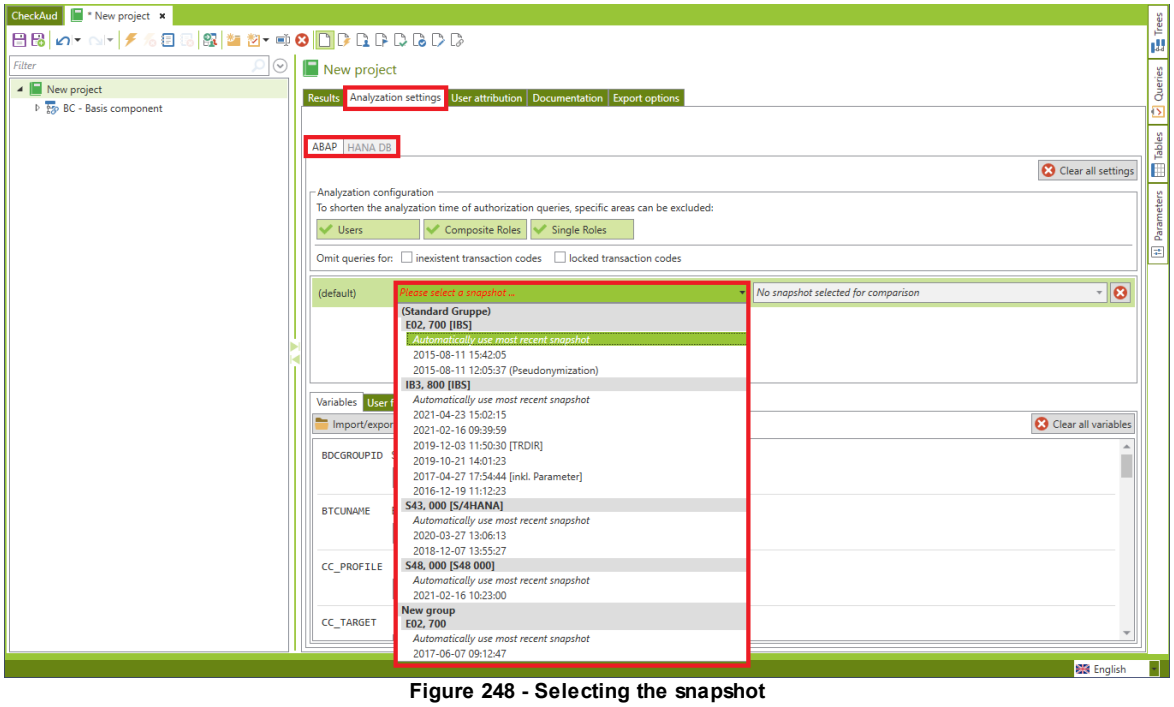



**Figure 248 - Selecting the snapshot**

Once the first two steps are complete, you can continue designing the new analysis project.

## V - 1.1 Creating new elements in the analysis project

You can create the following elements in an analysis project:

New folder

Folders constitute the organizational containers within the project. A folder can inherit settings or be assigned with new analysis settings by interrupting the inheritance. These new settings are then inherited to its subelements. The element can be given any name in German or English.

Query (ABAP)

The query is the technical check of (fully customizable) combinations of authorization objects that a SAP user may receive due to his or her assigned roles, profiles or reference users. This query generally covers a risk that can be quantified by the check, including the assessments defined in the query. The element can be given any name in German or English.

Query (HANA DB)

The query is the technical check of (fully customizable) combinations of authorization types that a HANA DB user may receive due to his or her assigned roles. This query generally covers a risk that can be quantified by the check, including the assessments defined in the query. The element can be given any name in German or English.

To create these elements, you must select the project in the menu bar, you can then use the buttons

Create a new folder in the analysis project

Create a new query in the analysis project

to create your desired element:

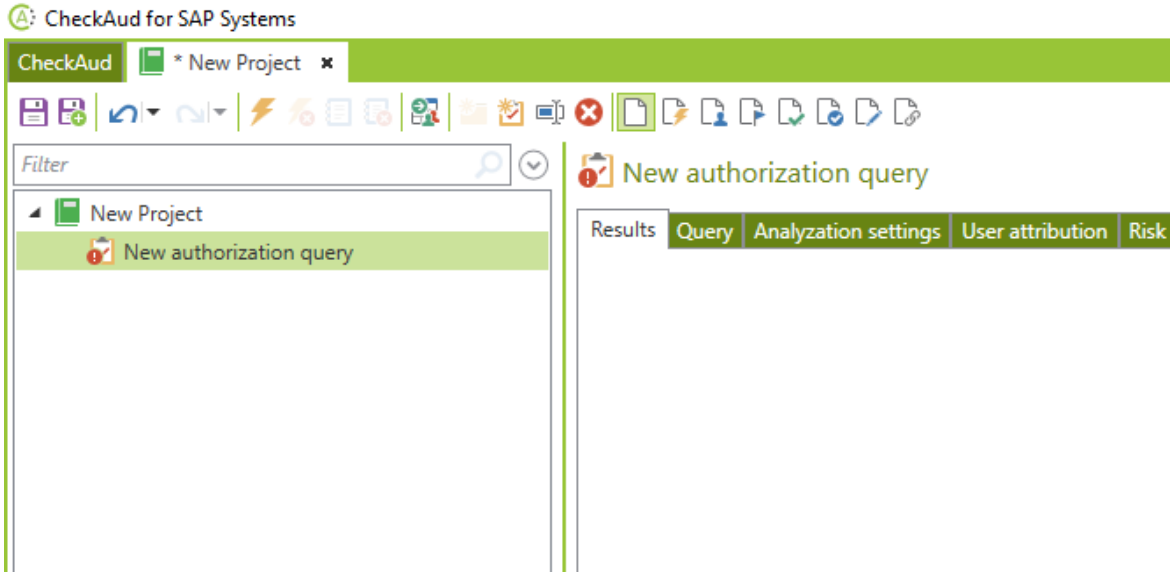



**Figure 249 - Creating new elements in your own analysis project**

Alternatively, you can also use the context menu in the analysis project to create new elements:

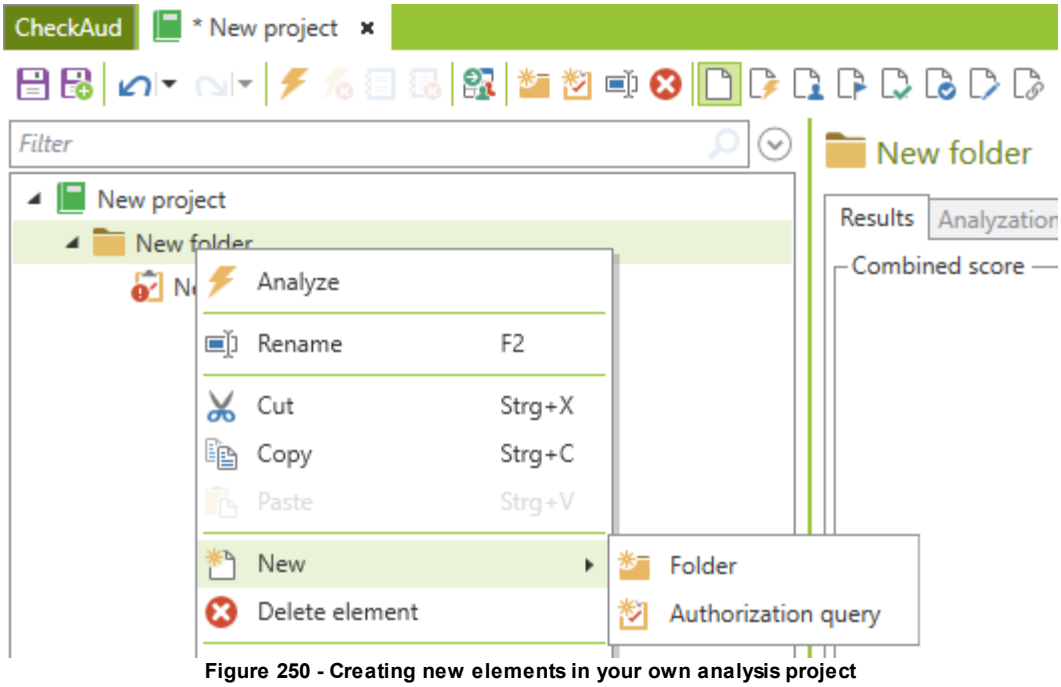



**Figure 250 - Creating new elements in your own analysis project**

**Note:** The new authorization query element in the analysis project is still empty; this means that you have not yet defined authorization objects to be checked for this authorization query. This is indicated by the exclamation mark on the icon.

## V - 1.2 Renaming new elements in the analysis project

You can rename your newly created elements. You must select the element in question to do so. You can use the button *Rename the current selected element* in the analysis project to rename the element. The languages German and English are provided by default. For detailed information about using multiple languages in your analysis project, see the chapter *Analysis Projects*.

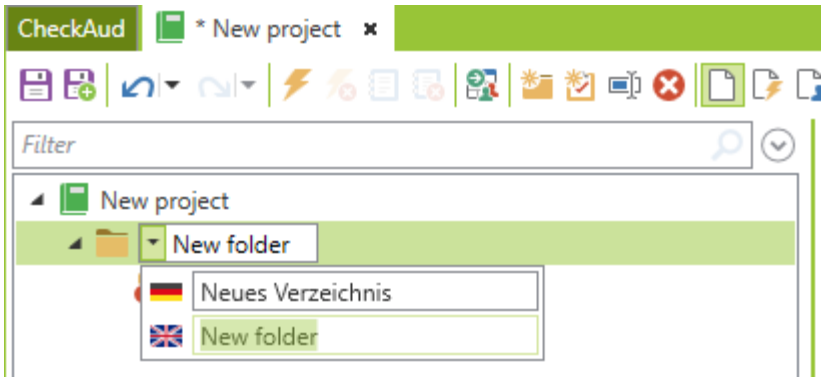



**Figure 251 - Renaming elements**

Alternatively, you can also use the context menu in the analysis project to rename new elements:

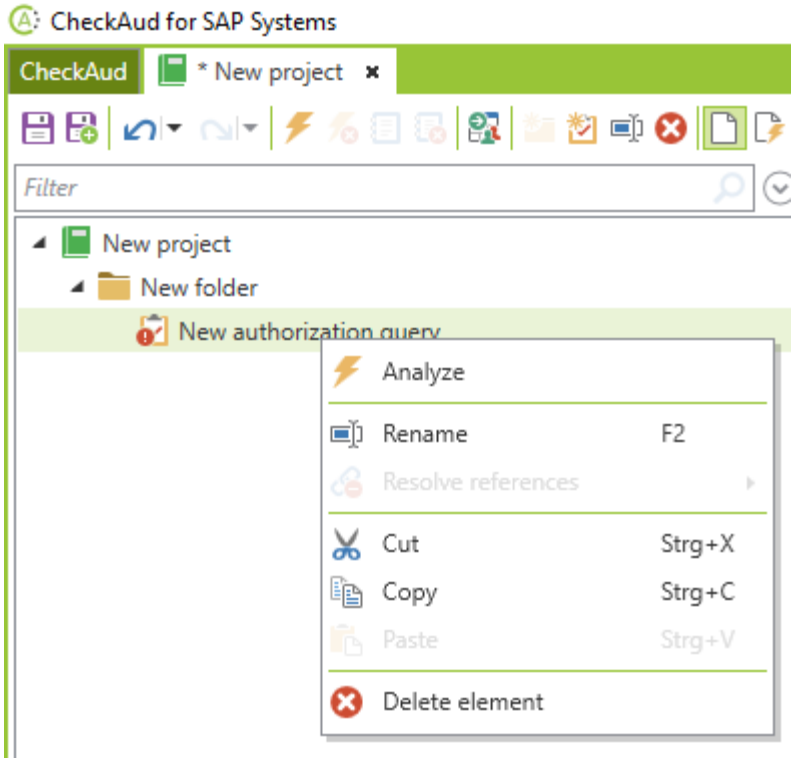
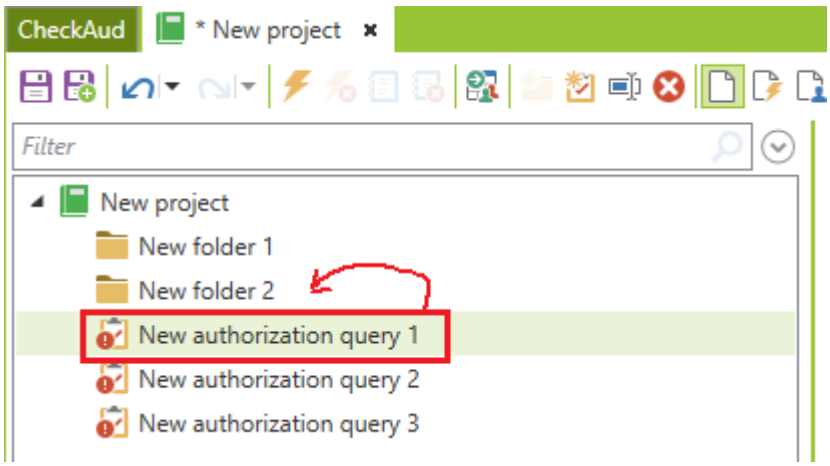



**Figure 252 - Renaming elements**

## V - 1.3 Moving and arranging new elements in the analysis project

You can move and rearrange elements within the structures in the analysis tree using drag and drop. If you drag and drop an element on a folder, the element in question becomes a subelement of the folder:



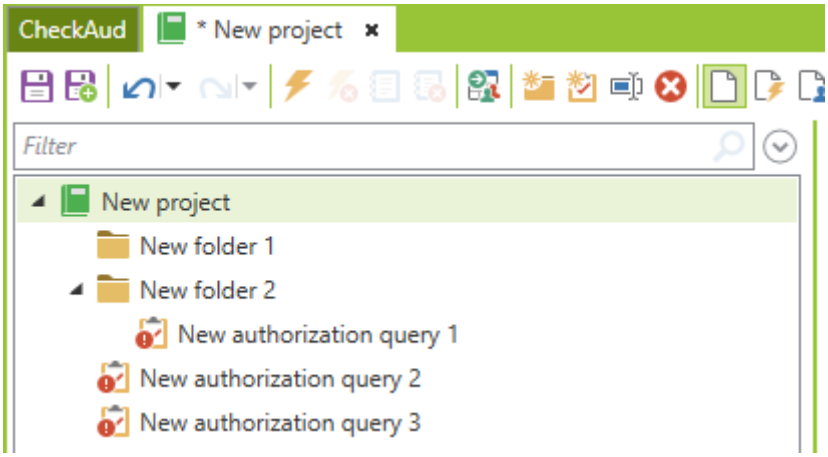
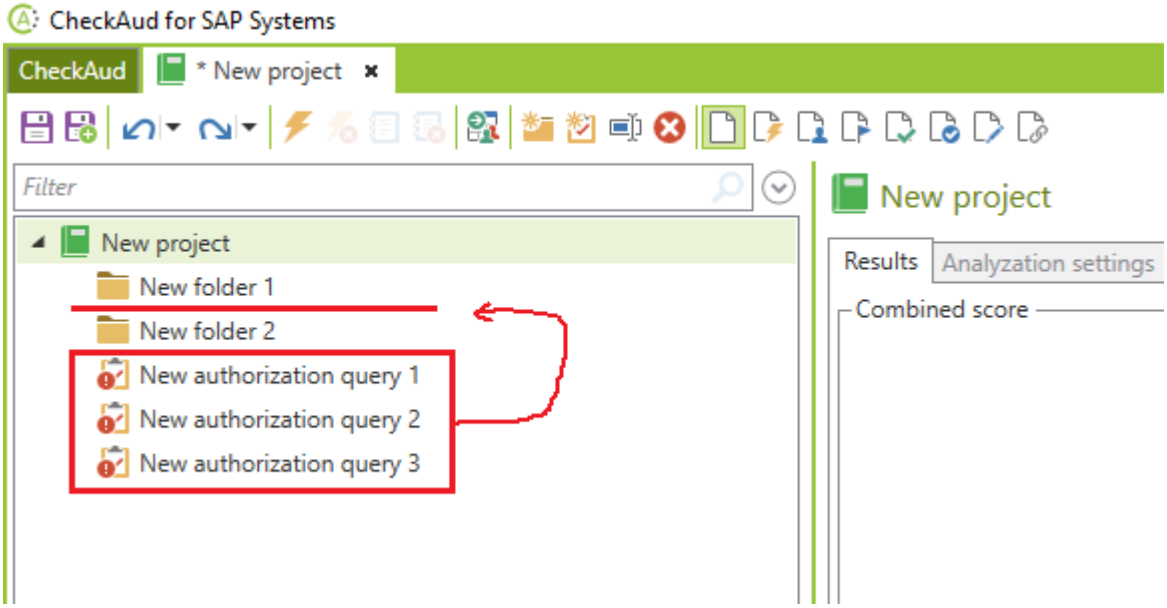



**Figure 253 - Structuring a project using drag and drop**

If you drop an element on the higher-level folder or the project, the element in question is then added to the folder or project as the last element. This allows you to arrange the elements in the project:



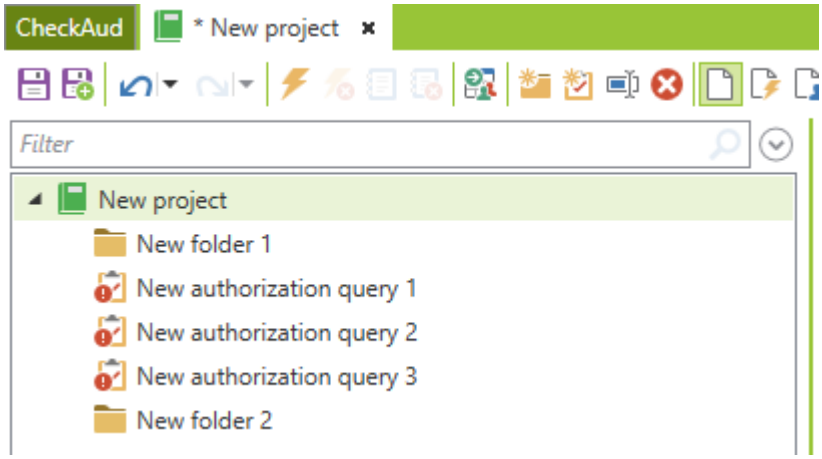
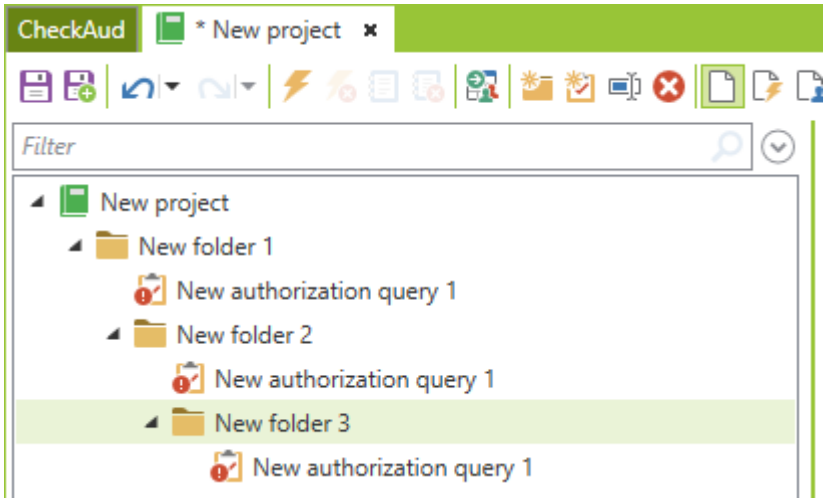



**Figure 254 - Arranging elements using drag and drop**

## V - 1.4 Deleting elements in the analysis project

You can use the button *Delete the current selected element* in the analysis project to delete the currently selected analysis project elements. When you select and delete a directory, all the subelements in the directory are also deleted immediately.



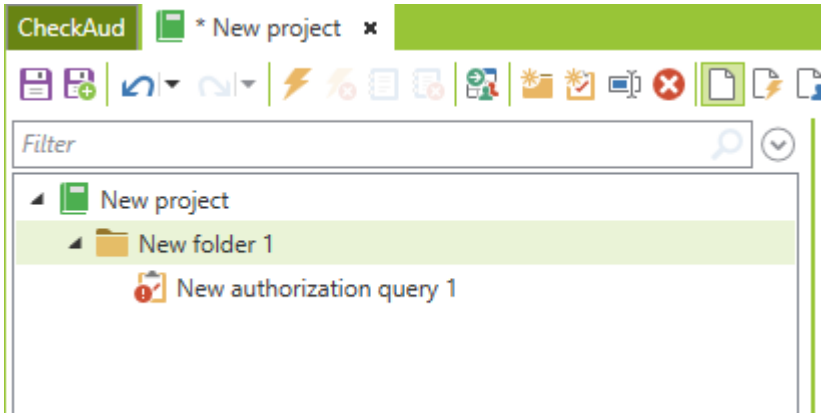



**Figure 255 - Deleting elements**

Alternatively, you can perform the deletion using the corresponding context menu item.

# V - 2 Using template projects

## V - 2.1 Template projects

The standard authorization queries, table queries and parameter checks provided by IBS Schreiber GmbH are sorted by theme in templates. You can use these templates or parts of them in your own analysis projects. The following analysis tree templates are currently available in CheckAud:

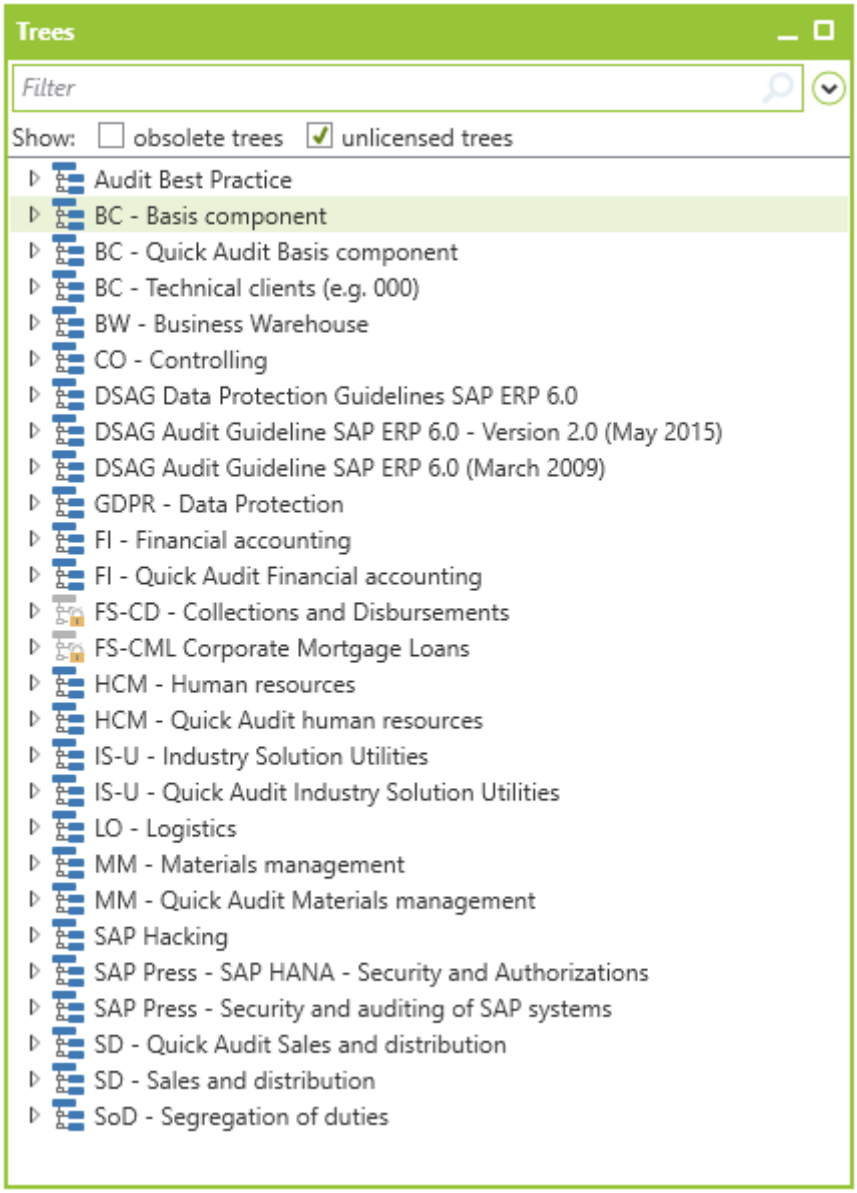



**Figure 256 - Supplied standard templates**

## V - 2.2 Licensed template projetcs

According to the used license not all of the template projects will be available. You can identify usable content with symbols in the Trees or Query toolbox.
I

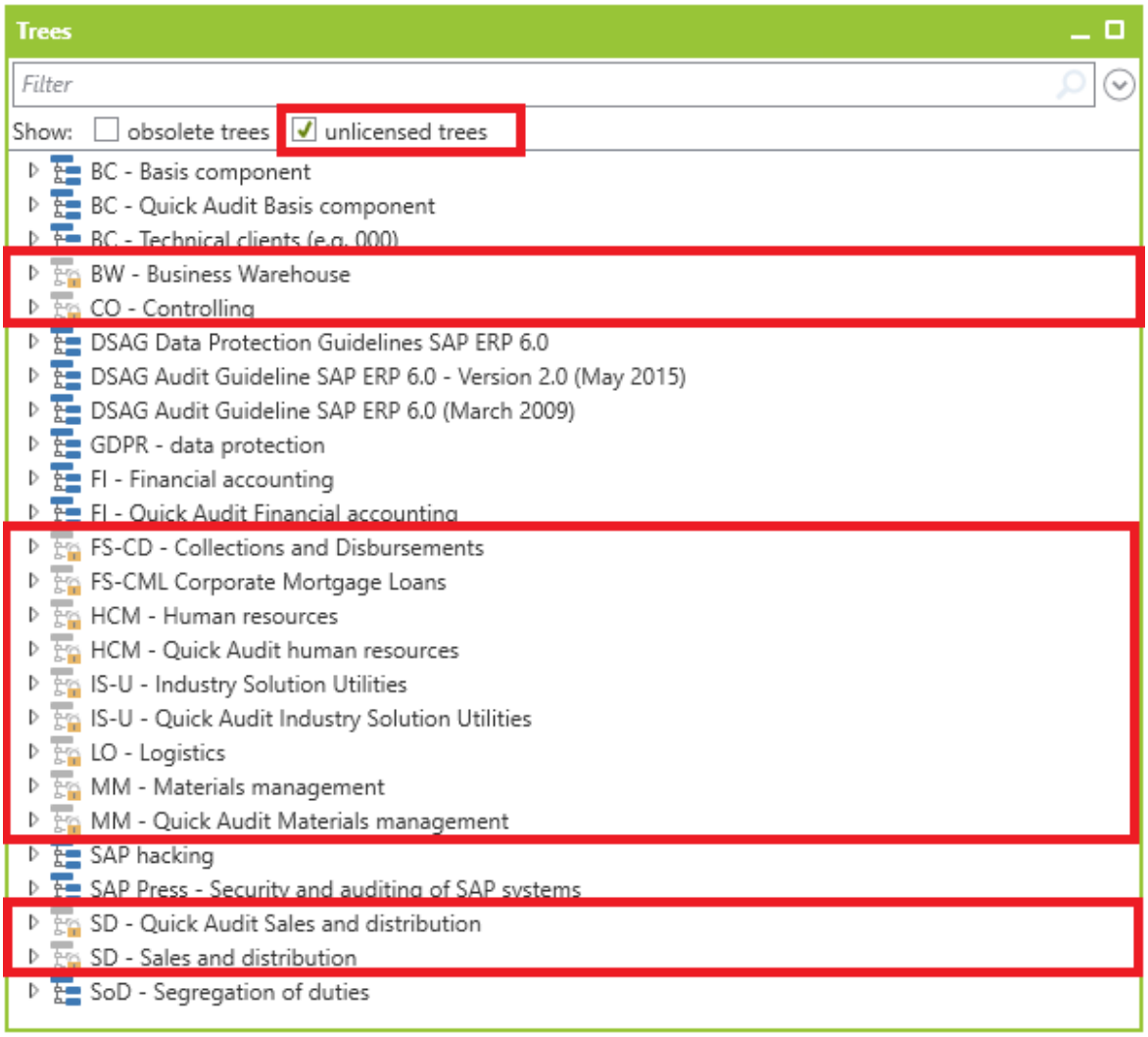



**Figure 257 - Licensed template projects**

| | |
|---|---|
| | template project is available with the used license |
| | template project is not available with the used license |

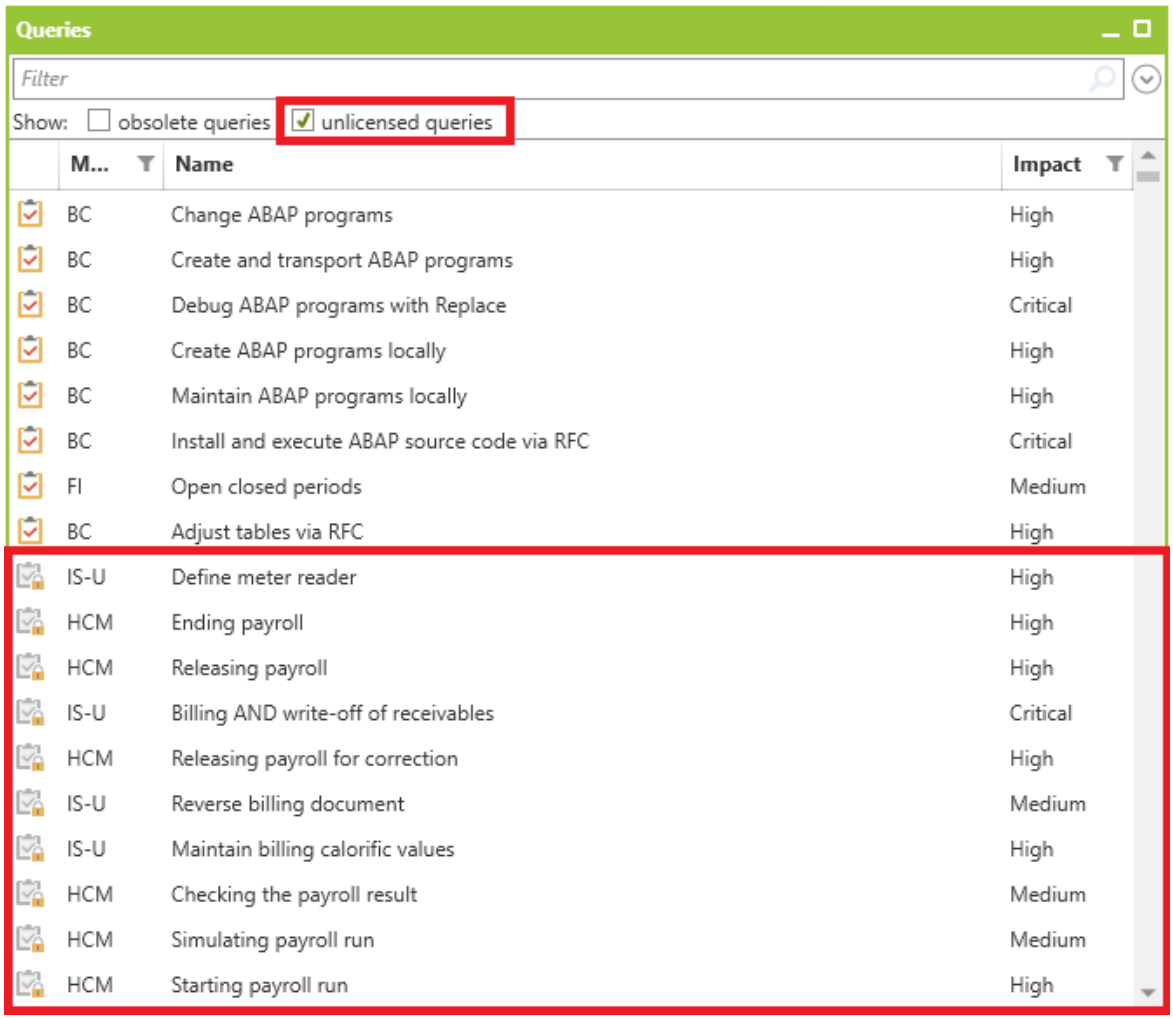



**Figure 258 - Licensed queries**

| | |
|---|---|
| | query is available with the used license |
| | query is not available with the used license |

Unlicensed content will be shown but is not useable for own analysis projects.

To check, which content will be delivered with your license, you can use the *About CheckAud* menu:


**Abbildung 259 - Lizenzinhalte**

| | |
|---|---|
| *Content* | The content delivered with the license will be shown here<br>- project template is delivered with the license and can be used in projects<br>- project template is not delivered with the license and can't be used in projects |

## V - 2.3 Obsolete template projects / queries

The authorization queries supplied in CheckAud are subject to constant and extensive improvement, which is vital due to the developments and changes in the SAP system. The templates and the queries that they contain are constantly updated and amended based on new knowledge acquired from the activities of IBS and the feedback received from CheckAud users. It is therefore inevitable that templates and the queries they contain may need to be restructured and, if necessary, replaced.

To ensure that old templates and the queries they contain can continue to be used, they are flagged as obsolete as opposed to being deleted. They are no longer displayed under the *Trees* and *Queries* tabs by default, but can be displayed additionally.

You can display obsolete trees and queries by clicking the *Show obsolete trees* checkbox or the *Show obsolete queries* checkbox. The obsolete trees and queries are displayed in gray and can now be accessed using the filter (keyword search).

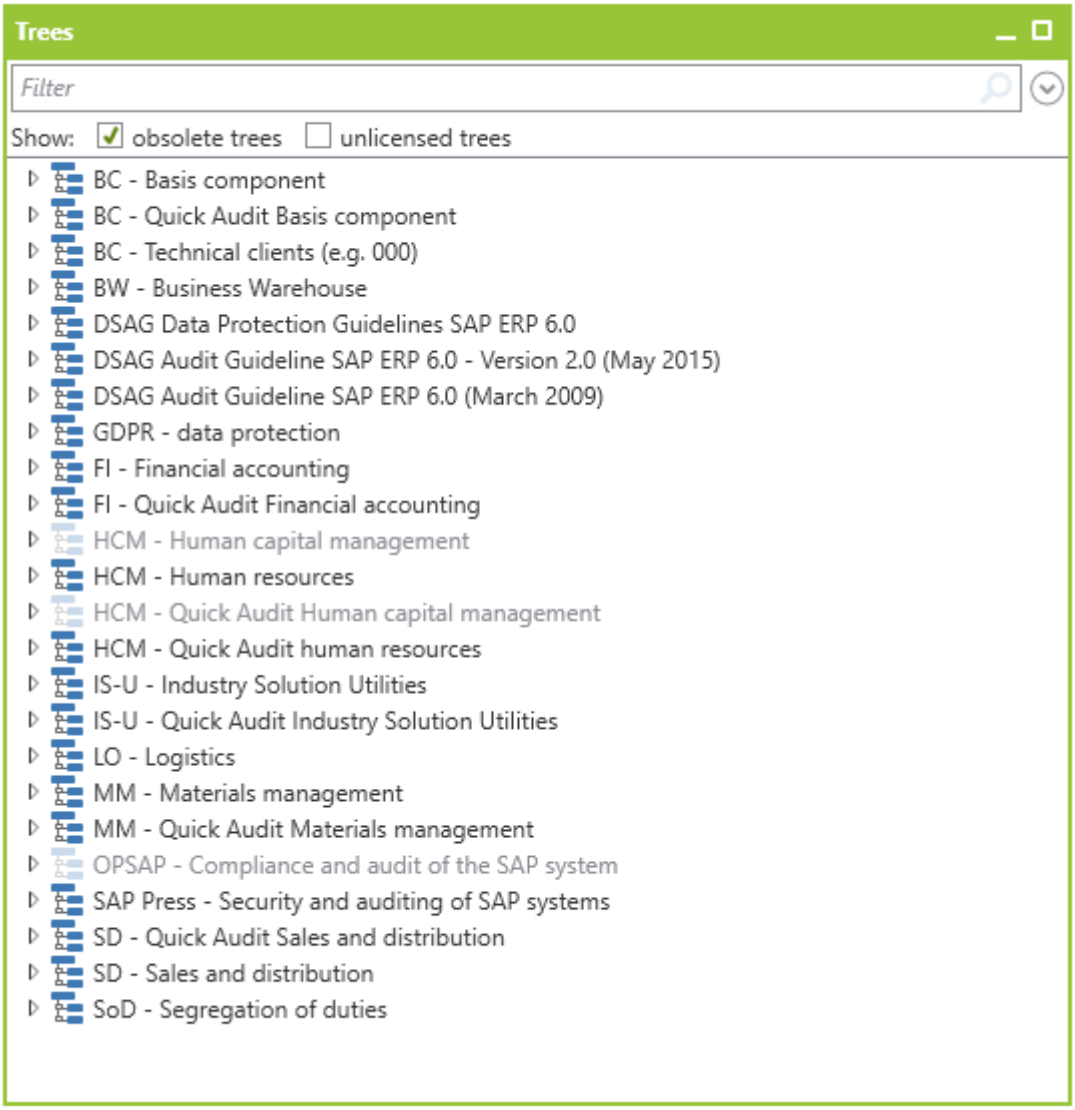



**Figure 260 - Obsolete template projects**

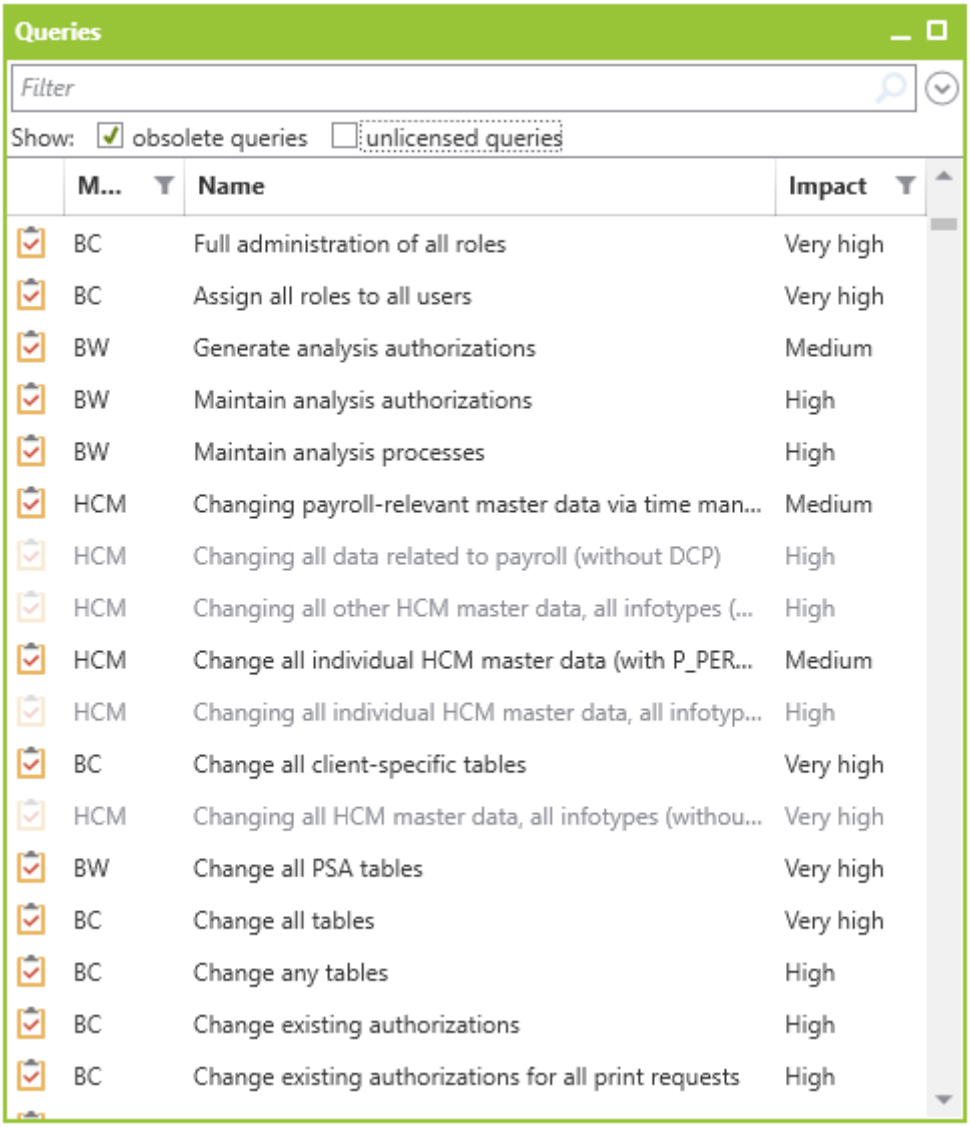



**Figure 261 - Obsolete queries**

## V - 2.4 Recommended table sets for using templates (ABAP & HANA DB)

Die ausgelieferten Vorlagenbäume für ABAP- und HANA DB-Prüfungen enthalten u. U. Abfragen auf Tabellen und Parameter, welche nicht im Standard-Tabellen-Set enthalten sind. Um dennoch alle Abfragen der Vorlagenbäume verwenden zu können, sollten bei der Erstellung der Snapshots gemäß nachfolgender Auflistung die optionalen Tabellen-Sets mit aktiviert werden:

| Name des Vorlagenbaumes | Standard-Set | Zusätzliche Sets | Parameter |
|---|---|---|---|
| Audit Best Practice | AUTH (ABAP) | IBS_SYSTEM (ABAP), IBS_AUTH_ADVANCED, | ja |

| | | | |
|---|---|---|---|
| | | IBS_FI, IBS_MM, IBS_SD, IBS_BW, IBS_HCM | |
| BC - Basis | AUTH (ABAP) | IBS_SYSTEM (ABAP), IBS_AUTH_ADVANCED | ja |
| BC - Schnellprüfung Basis | AUTH (ABAP) | IBS_SYSTEM (ABAP) | ja |
| BC - Technische Mandaten (z.B. 000) | AUTH (ABAP) | IBS_SYSTEM (ABAP) | nein |
| BW - Business Warehouse | AUTH (ABAP) | IBS_BW | nein |
| CO - Controllling | AUTH (ABAP) | IBS_CO | nein |
| DSAG Datenschutzleitfaden SAP ERP 6.0 | AUTH (ABAP) | IBS_SYSTEM (ABAP) | ja |
| DSAG Prüfleitfaden SAP ERP 6.0 - Version 2.0 (Mai 2015) | AUTH (ABAP) | IBS_SYSTEM (ABAP) | ja |
| DSAG Prüfleitfaden SAP ERP 6.0 (März 2009) | AUTH (ABAP) | IBS_SYSTEM (ABAP) | ja |
| DSGVO - Datenschutz | AUTH (ABAP) | IBS_GDPR | ja |
| FI - Finanzbuchhaltung | AUTH (ABAP) | IBS_FI | ja |
| FI - Schnellprüfung Finanzbuchhaltung | AUTH (ABAP) | IBS_FI | nein |
| FS-CD - In- und Exkasso | AUTH (ABAP) | - | nein |
| FS-CML Corporate Mortgage Loans | AUTH (ABAP) | - | nein |
| HCM - Personalwesen | AUTH (ABAP) | IBS_HCM, IBS_SYSTEM (ABAP) | nein |
| HCM - Schnellprüfung Personalwesen | AUTH (ABAP) | IBS_HCM, IBS_SYSTEM (ABAP) | nein |
| IS-U - Industry Solution Utilities | AUTH (ABAP) | IBS_ISU | nein |
| IS-U - Schnellprüfung Industry Solution Utilities | AUTH (ABAP) | IBS_ISU | nein |
| LO - Logistik | AUTH (ABAP) | - | nein |
| MM - Materialwirtschaft | AUTH (ABAP) | IBS_MM | nein |
| MM - Schnellprüfung Materialwirtschaft | AUTH (ABAP) | IBS_MM | nein |
| RE-FX - Flexibles Immobilienmanagement | AUTH (ABAP) | - | nein |
| SAP Hacking | AUTH (ABAP) | IBS_SYSTEM (ABAP), IBS_AUTH_ADVANCED | ja |
| SAP HANA - Cockpit | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |

| | | | |
|---|---|---|---|
| SAP HANA - ERP-/S/4HANA-Tenant | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP HANA - System-DB | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP Press - SAP HANA - Sicherheit und Berechtigungen | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP Press – Sicherheit und Prüfung von SAP-Systemen | AUTH (ABAP) | IBS_SYSTEM (ABAP) | ja |
| SD - Schnellprüfung Vertrieb | AUTH (ABAP) | IBS_SD | nein |
| SD - Vertrieb | AUTH (ABAP) | IBS_SD | nein |
| SOD - Funktionstrennung | AUTH (ABAP) | IBS_FI, IBS_MM, IBS_SD | nein |

----------OLD_TEXT----------
The supplied templates sometimes contain ABAP nad HANA DB queries of tables and parameters that are not included in the standard table set. To ensure that you can still use all the template queries regardless, you should also activate the optional table sets based on the list below when creating the snapshots:

| Name of template project | Standard sets | Additional sets | Parameter |
|---|---|---|---|
| Audit Best Practice | AUTH (ABAP) | IBS_SYSTEM (ABAP), IBS_AUTH_ADVANCED, IBS_FI, IBS_MM, IBS_SD, IBS_BW | yes |
| BC - Basis Components | AUTH (ABAP) | IBS_SYSTEM (ABAP), IBS_AUTH_ADVANCED | yes |
| BC - Quick Audit Basis | AUTH (ABAP) | IBS_SYSTEM (ABAP) | yes |
| BC - technical clients (e.G. 000) | AUTH (ABAP) | IBS_SYSTEM (ABAP) | no |
| BW - Business Warehouse | AUTH (ABAP) | IBS_BW | no |
| CO - Controllling | AUTH (ABAP) | IBS_CO | no |
| DSAG Data protection guidelines SAP ERP 6.0 | AUTH (ABAP) | IBS_SYSTEM (ABAP) | yes |
| DSAG Audit guideline SAP ERP 6.0 - Version 2.0 (May 2015) | AUTH (ABAP) | IBS_SYSTEM (ABAP) | yes |
| DSAG Audit guideline SAP ERP 6.0 (March 2009) | AUTH (ABAP) | IBS_SYSTEM (ABAP) | yes |
| GDPR - Data protection | AUTH (ABAP) | IBS_GDPR | yes |
| FI - Financial accounting | AUTH (ABAP) | IBS_FI | yes |

| | | | |
|---|---|---|---|
| FI - Quick audit financial accounting | AUTH (ABAP) | IBS_FI | no |
| FS-CD - Charge and Disbursement | AUTH (ABAP) | - | no |
| FS-CML Corporate Mortgage Loans | AUTH (ABAP) | - | no |
| HCM - Human resources | AUTH (ABAP) | IBS_HCM, IBS_SYSTEM (ABAP) | no |
| HCM - Quick audit human resources | AUTH (ABAP) | IBS_HCM, IBS_SYSTEM (ABAP) | no |
| IS-U - Industry Solution Utilities | AUTH (ABAP) | IBS_ISU | no |
| IS-U - Quick audit Industry Solution Utilities | AUTH (ABAP) | IBS_ISU | no |
| LO - Logistics | AUTH (ABAP) | - | no |
| MM - Material management | AUTH (ABAP) | IBS_MM | no |
| MM - Quick audit material management | AUTH (ABAP) | IBS_MM | no |
| RE-FX - Real Estate Management | AUTH (ABAP) | - | no |
| SAP Hacking | AUTH (ABAP) | IBS_SYSTEM (ABAP), IBS_AUTH_ADVANCED | yes |
| SAP HANA - Cockpit | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP HANA - ERP-/S/4HANA-Tenant | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP HANA - System-DB | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP Press - SAP HANA - Security and Authorizations | AUTH (HANA DB) | IBS_SYSTEM (HANA DB) | - |
| SAP Press – Security and auditing of SAP systems | AUTH (ABAP) | IBS_SYSTEM (ABAP) | yes |
| SD - Quick audit sales and distribution | AUTH (ABAP) | IBS_SD | no |
| SD - sales and distribution | AUTH (ABAP) | IBS_SD | no |
| SOD - Segregation of duties | AUTH (ABAP) | IBS_FI, IBS_MM, IBS_SD | no |

## V - 2.5 Referencing a template project

To integrate (reference) a template in your own project, you can drag the desired template from the toolbox and drop it in your project:

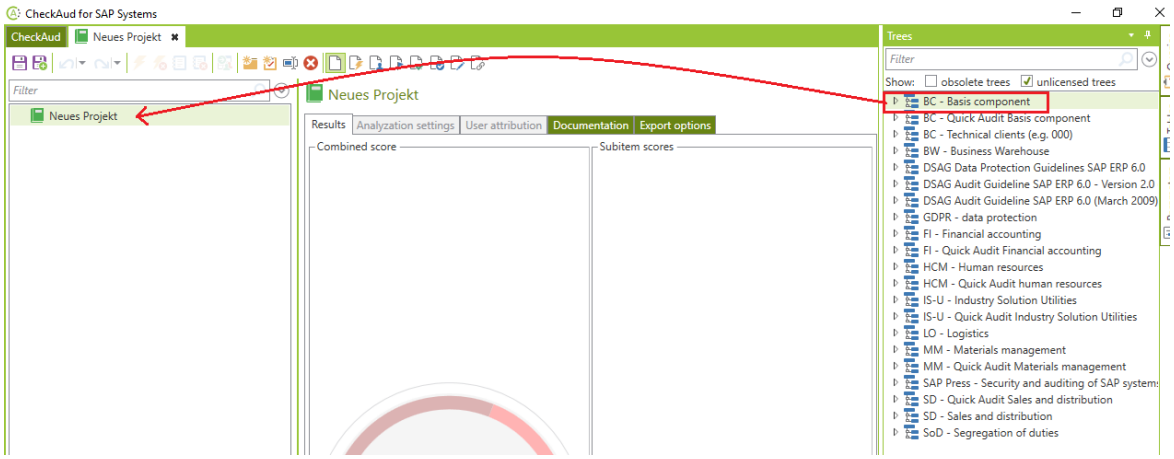



**Figure 262 - Adding a template to your project (as a reference)**

The template is then added to the project as a reference:

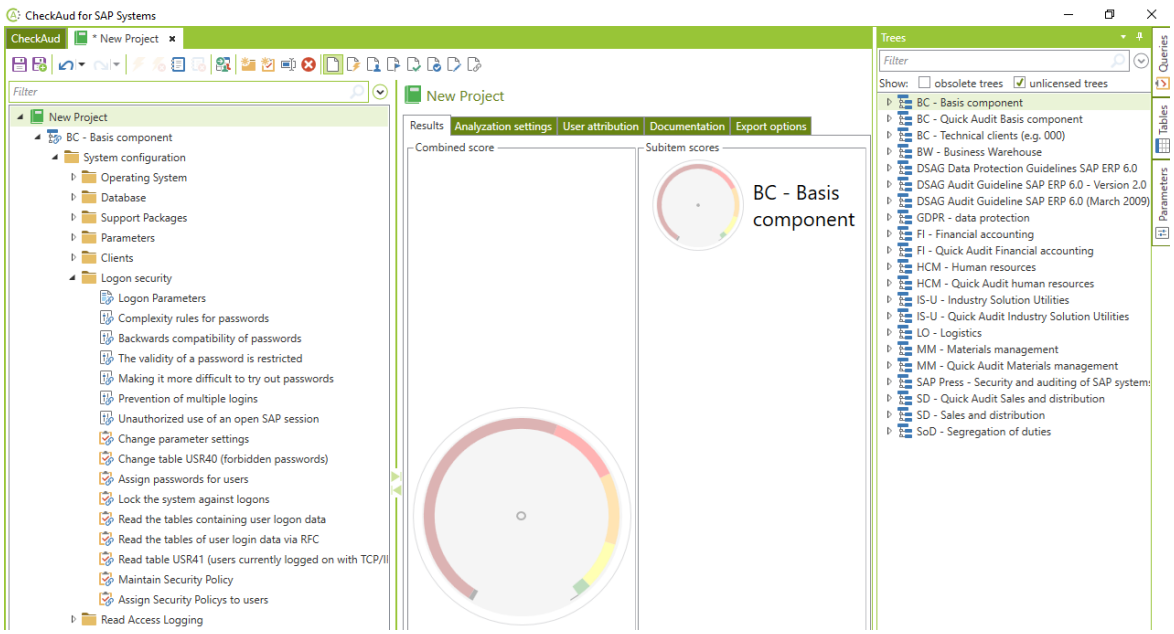



**Figure 263 - Added template**

The name of the individual elements and the general structure and composition of the contents in the referenced template cannot be changed. Only the risk management information (assessment, description, user assignment), filters and variables can be given custom definitions.

The template can be edited only after removing the reference. For information about removing the reference, see the chapter *Removing Query References*.

## V - 2.6 Referencing a part of a template project

Alternatively, you can also only include part of a template, including individual template queries, in your own project. Once again, you drag and drop it from the toolbox to do so:

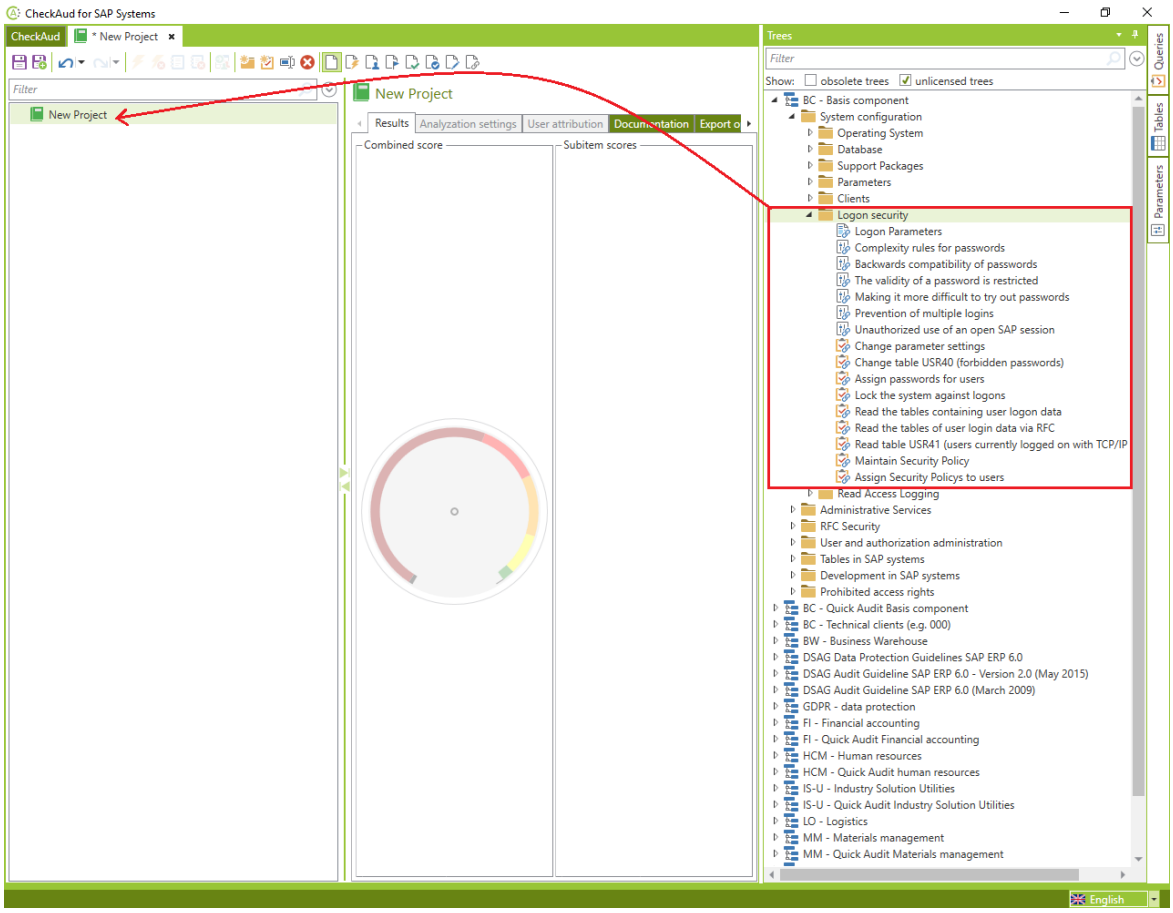



**Figure 264 - Adding part of a template to your project (as a reference)**

The relevant sub-template is then referenced in your analysis project:

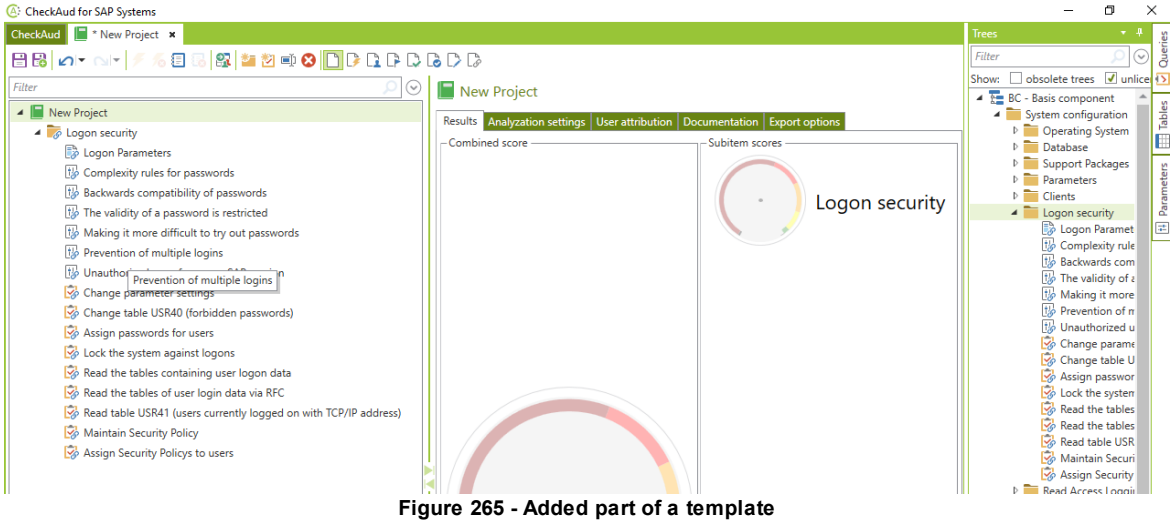



**Figure 265 - Added part of a template**

The name of the individual elements and the general structure and composition of the contents in the referenced part of the template cannot be changed. Only the risk management information (assessment, description, user assignment), filters and variables can be given custom definitions.

The template can be edited only after removing the reference. For information about removing the reference, see the chapter *Removing Query References*.

# V - 3 Authorization queries

Authorization queries are the cornerstone of the CheckAud auditing software. You can use the authorization queries in the standard IBS system (references) or fully create them yourself. A graphical editor and text editor are provided to do so.

## V - 3.1 IBS standard queries

You can use the toolbox to choose from the whole range of authorization queries delivered with the standard system and add them to your own analysis project. When doing so, you only set references in the analysis project, so that the composition and settings of these queries are automatically updated during IBS updates. The name and composition of referenced queries cannot be changed. Only the risk assessment, risk description and user assignment can be customized. You select an IBS standard query from the toolbox using drag and drop:

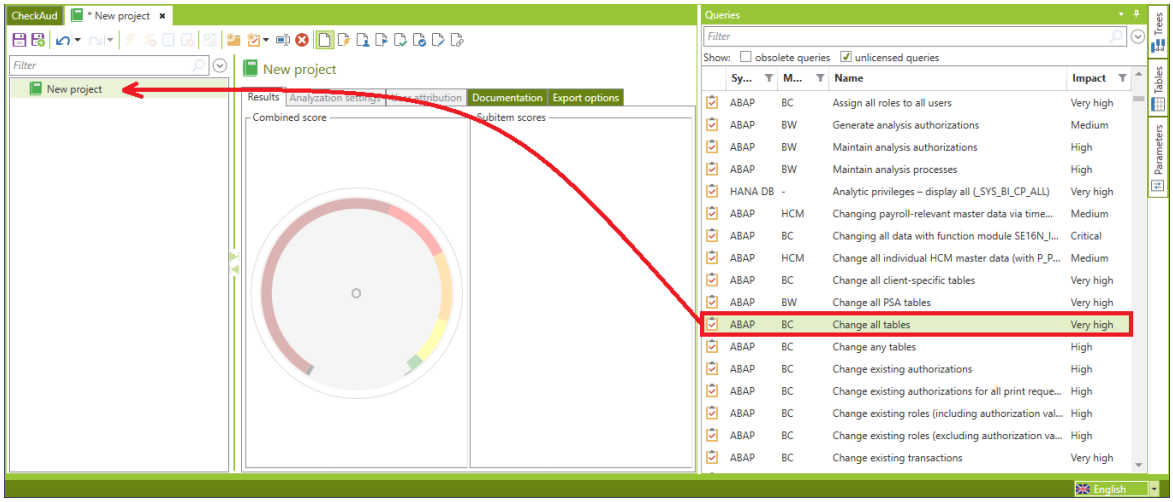
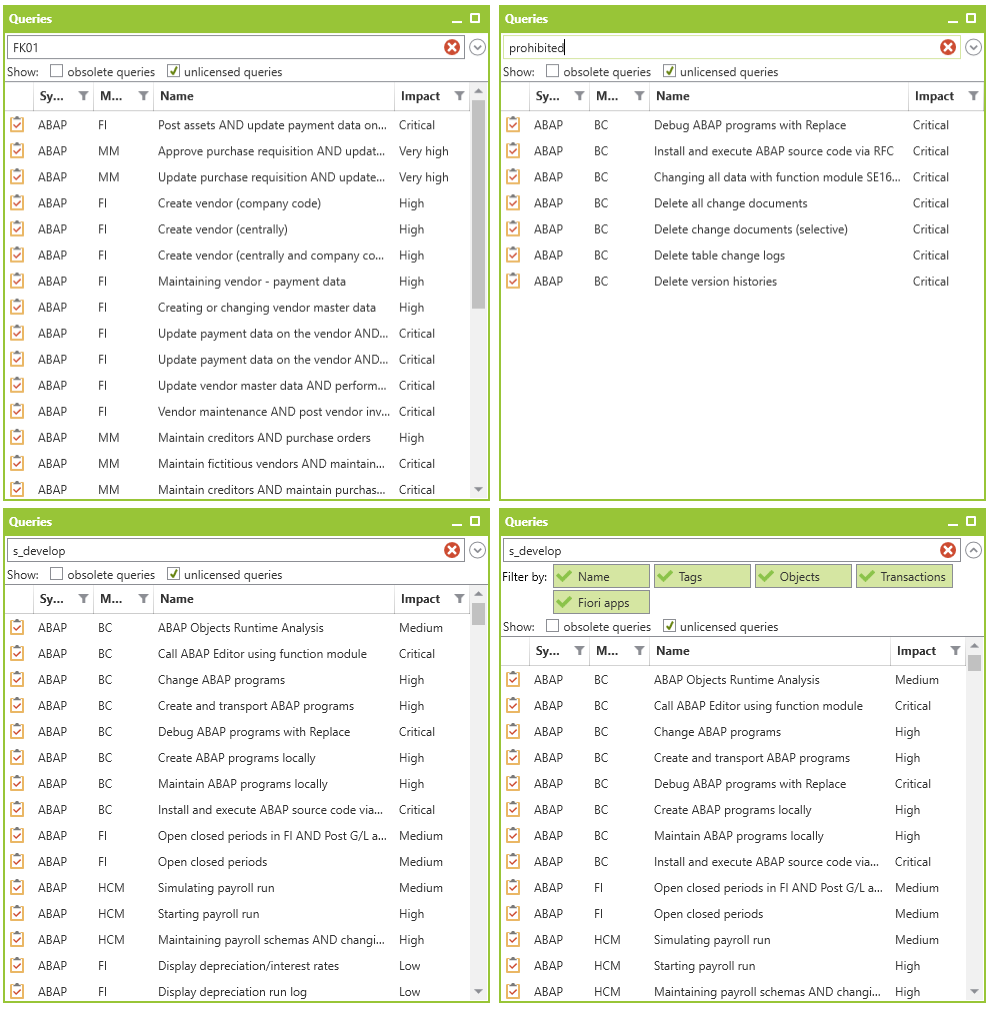



**Figure 266 - Adding IBS standard queries in the analysis project**

IBS standard queries are sorted in alphabetical order in the toolbox. You can also use the search field to search for specific queries. It allows you to search for criteria such as parts of a name, tags, transactions or authorization objects that are used in the queries:




Queries can be pre-selected for special modules or risk impacts. Therefore filters can be used to select single or multiple queries regarding their dependencies to modules or iompacts.

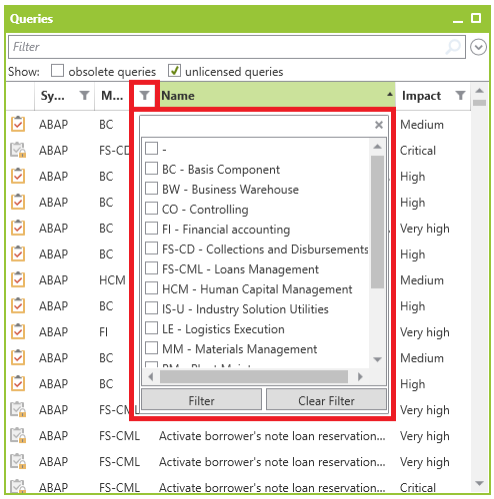



Figure 267 - Filter by module

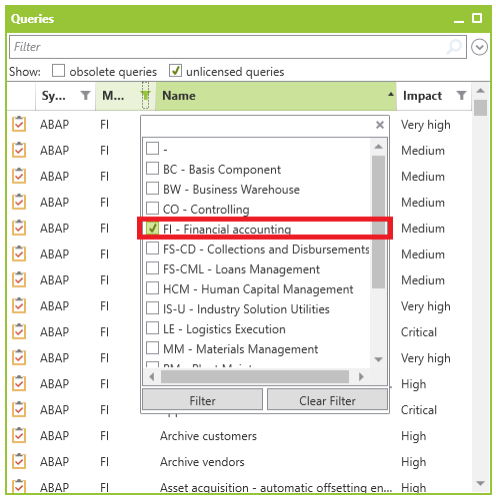



Figure 268 - Filter by modlue FI

Another possibiliy to pre-select queries is via risk impact. In this example it is possible to enlist any query which has a critical impact.

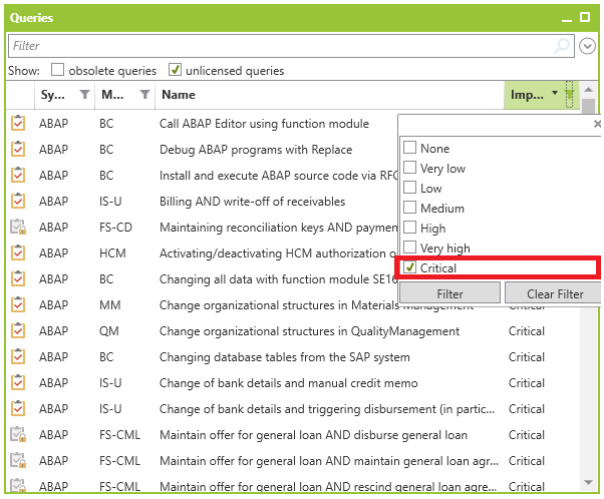



**Figure 269 - Filterung by impact**

Filters can be used single or in combination, for example to anlist queries from module financial accounting with a critical impact.

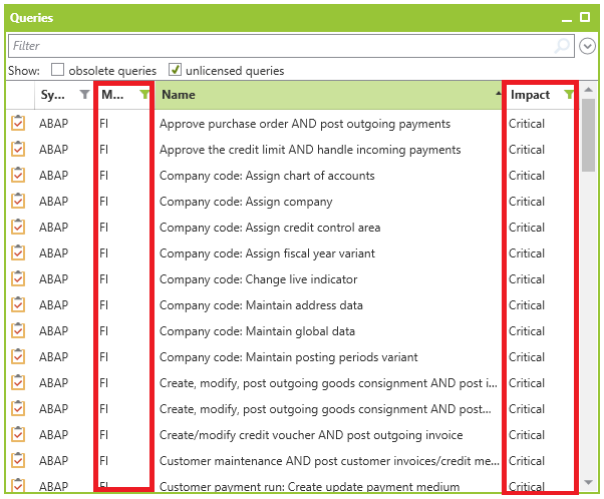



**Figure 270 - Filter by impact and module FI**

## V - 3.2 Preview of IBS standard queries

To view a query in more detail in the toolbox before adding it to the project tree, right-click the required standard query. Click the Details button to open a preview of the query.

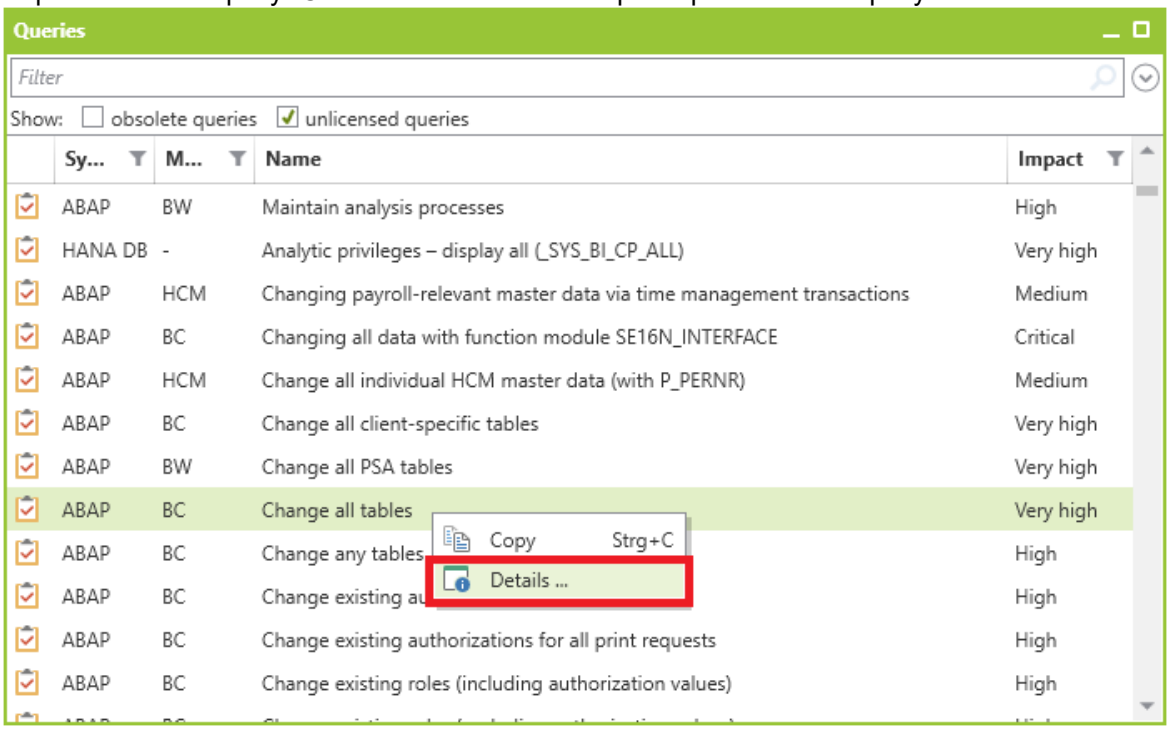



**Figure 271 - Opening the authorization query preview**

This preview shows the query syntax, risk management, and documentation.

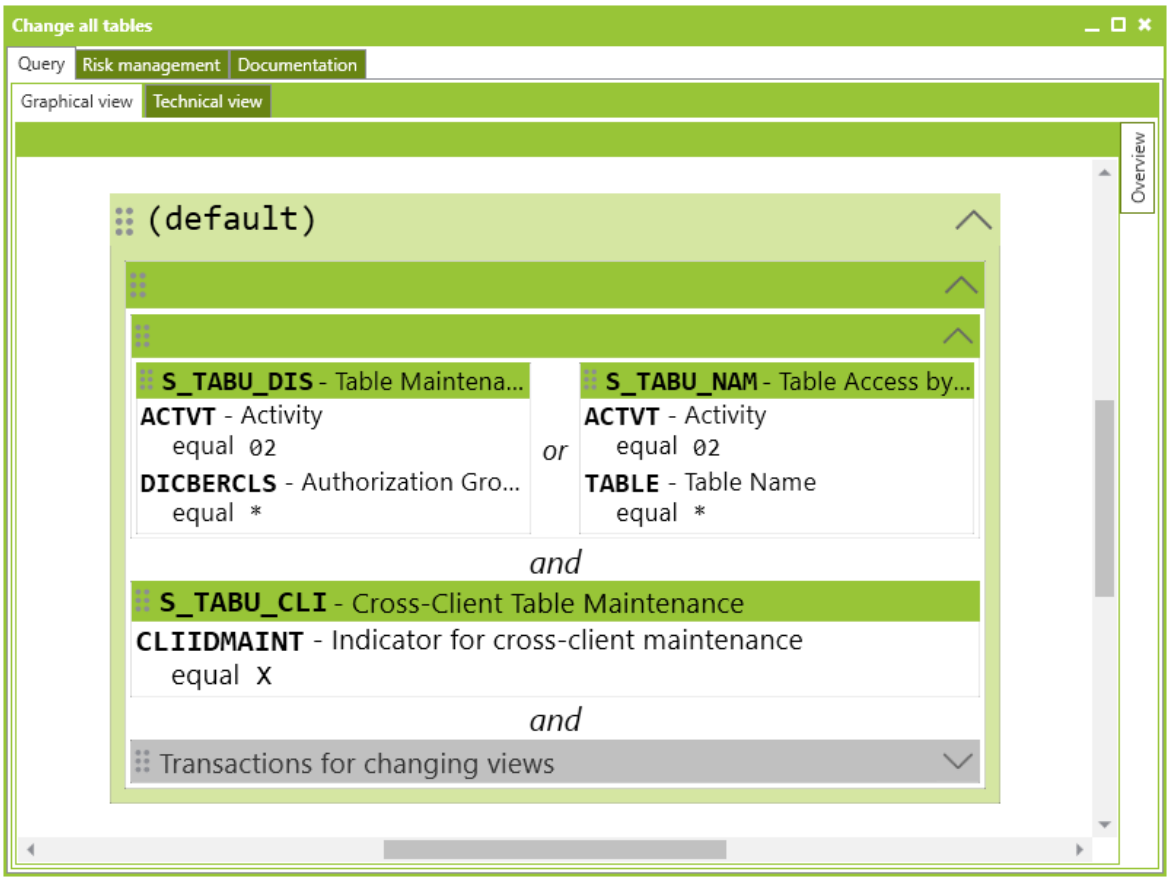



**Figure 272 - Displaying the preview**

## V - 3.3 Removing query references

To edit IBS standard queries that are referenced in the analysis project, you can disconnect them from the reference in the context menu.

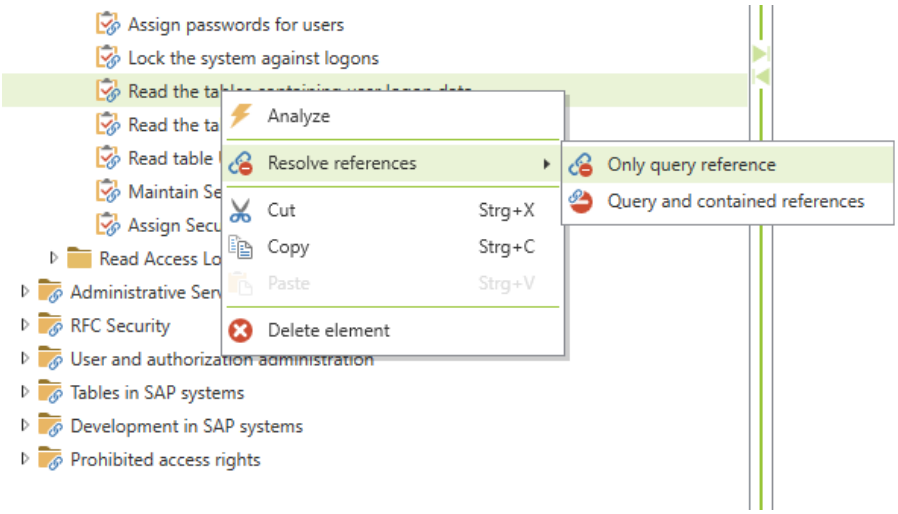



**Figure 273 - Removing a query reference**

The following functions are available to do this:

Query references can be converted into editable queries using the Only query reference function in the context menu:

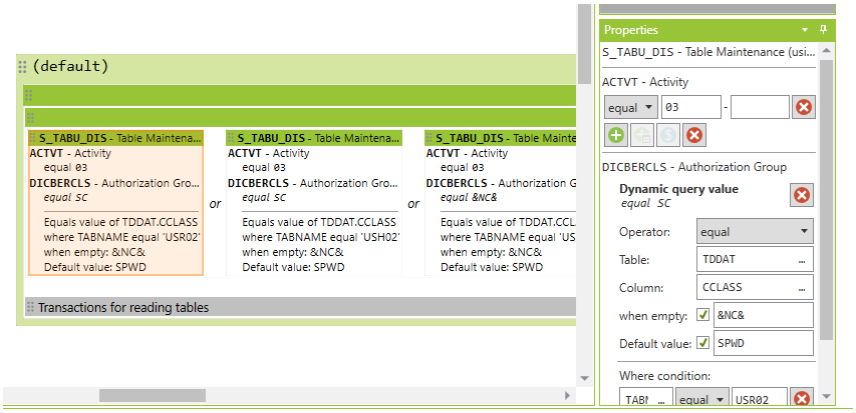
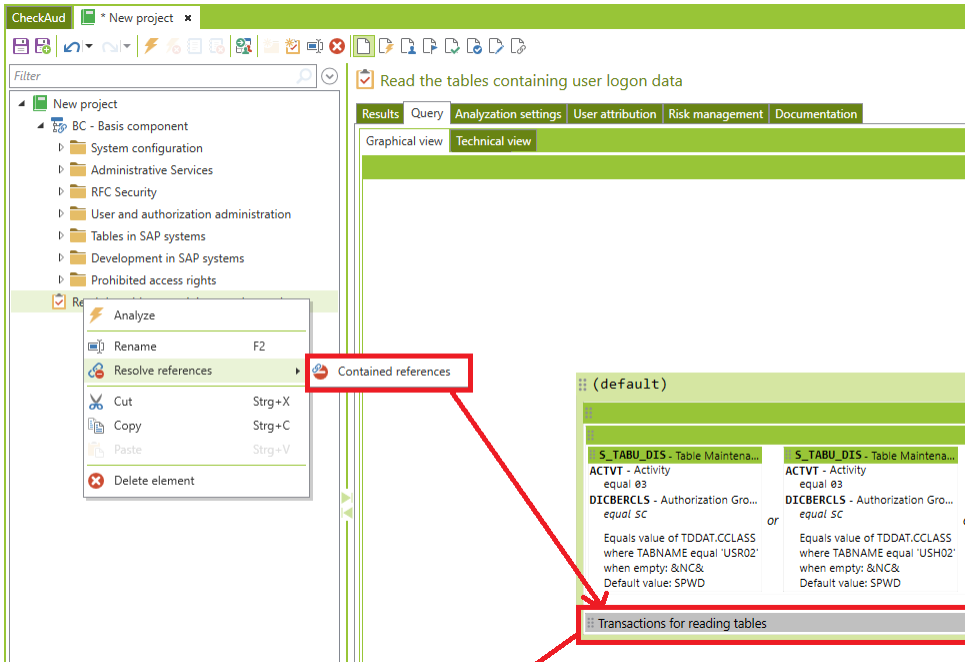
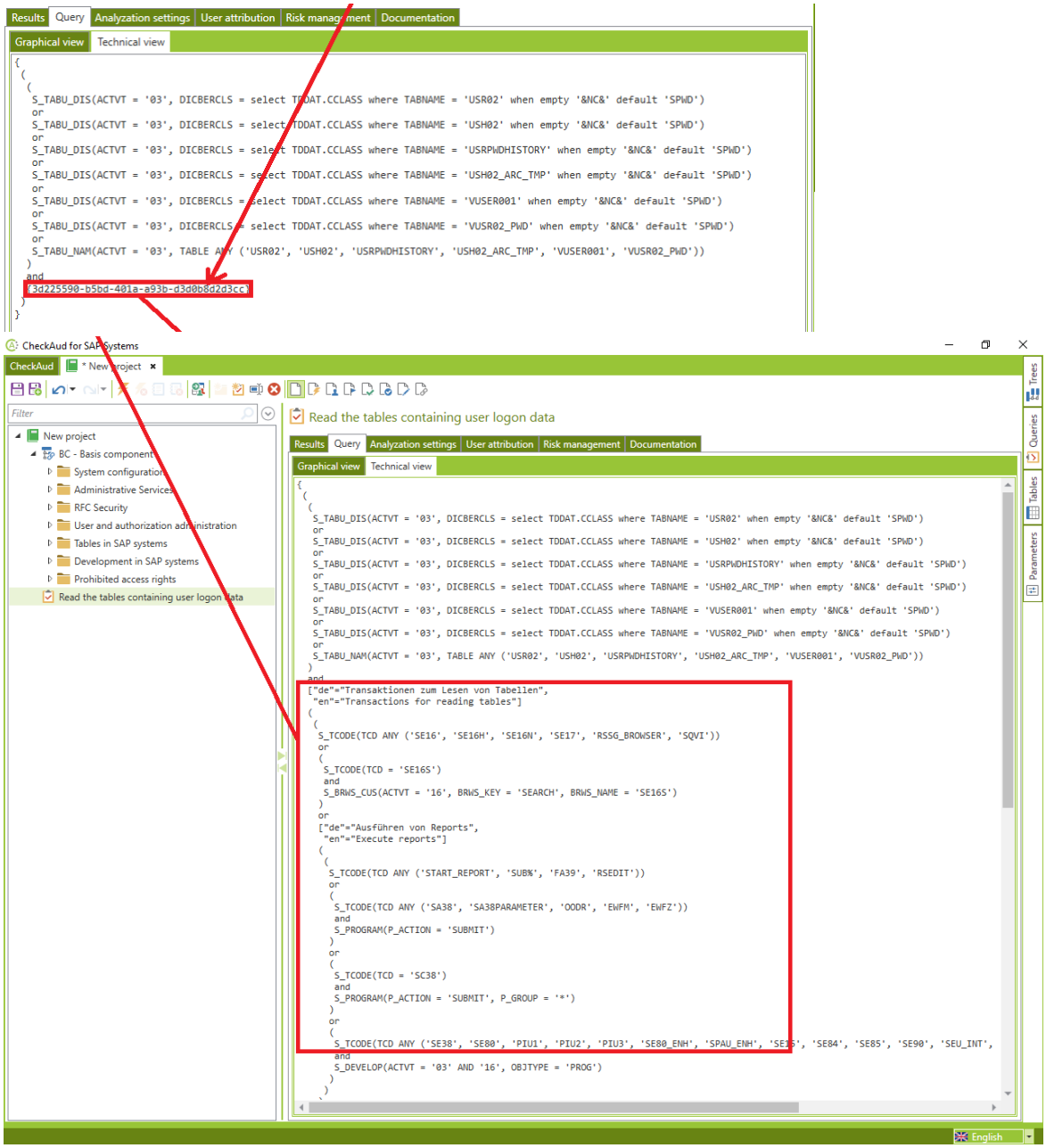



**Figure 274 - Removed, editable query reference**

The references contained in editable queries can be completely removed using Contained references in the context menu:


CheckAud
* New project
Filter
New project
BC - Basis component
System configuration
Administrative Services
RFC Security
User and authorization administration
Tables in SAP systems
Development in SAP systems
Prohibited access rights
Analyze
Rename F2
Resolve references
Cut Strg+X
Copy Strg+C
Paste Strg+V
Delete element
Contained references
Read the tables containing user logon data
Results
Query
Analyzation settings
User attribution
Risk management
Documentation
Graphical view
Technical view
(default)
S_TABU_DIS - Table Maintena...
ACTVT - Activity
equal 03
DICBERCLS - Authorization Gro...
equal SC
Equals value of TDDAT.CCLASS where TABNAME equal 'USR02' when empty: &NC&
Default value: SPWD
or
S_TABU_DIS - Table Maintena...
ACTVT - Activity
equal 03
DICBERCLS - Authorization Gro...
equal SC
Equals value of TDDAT.CCLASS where TABNAME equal 'USH02' when empty: &NC&
Default value: SPWD
Transactions for reading tables




The references contained in queries can also be resolved using the graphical editor:

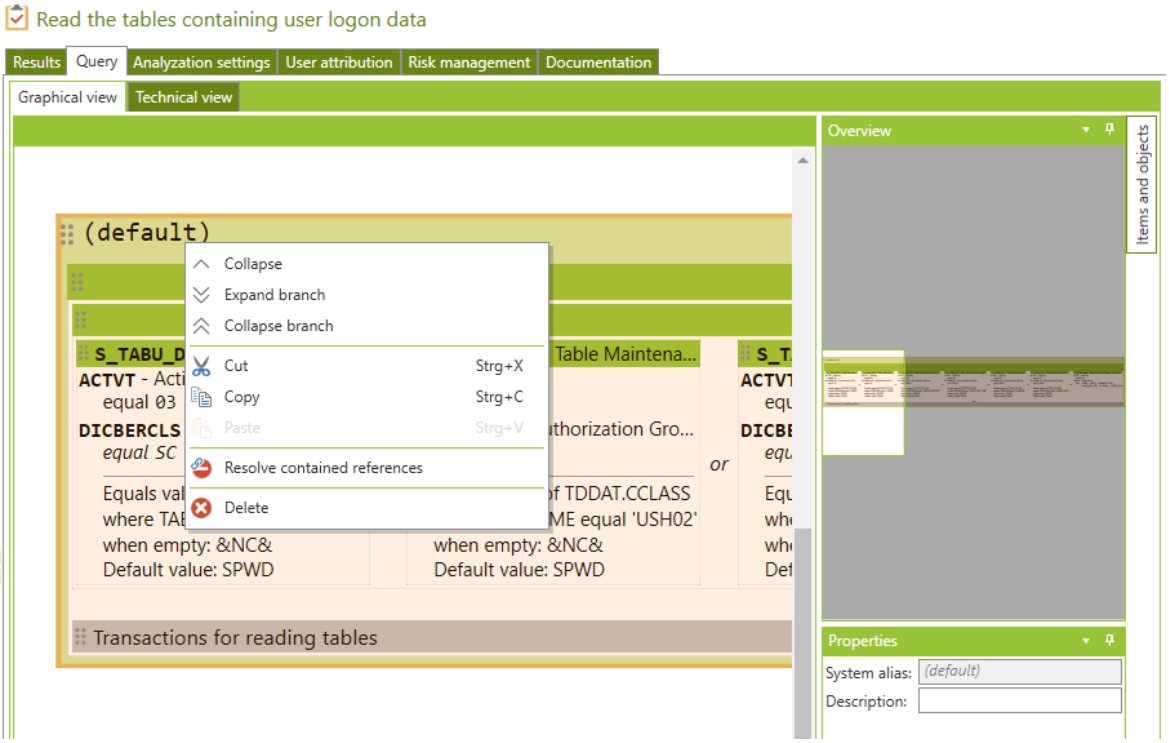



**Figure 275 - Removing a reference using the graphical editor**

When you right-click the button in the graphical editor, the context menu for the query opens. Here, you can remove the query reference if there is one.

Remove query reference; other contained references are not removed

Remove query reference together with all other contained references

You can use the Undo (Rückgängig) function in the quick access menu to restore the query to its original state.


**Figure 276 - Undoing your last actions**

**Note:** Predefined queries from the “Queries” toolbox can be immediately removed and added to your own project using drag and drop with the Ctrl key held down. Predefined analysis trees from the “Trees” toolbox can be pasted as a copy if you drag and drop them with the Ctrl key held down. This way, you can adjust the structure of the predefined analysis tree as needed. However, included references to queries are not cut and remain in the tree as a reference.

**Note:** Removed query references are not automatically updated during updates of the IBS standard queries!

To find not referenced queries in the analysis project easely, you can use the button to switch to a project view, which marks the not referenced elements in the project:

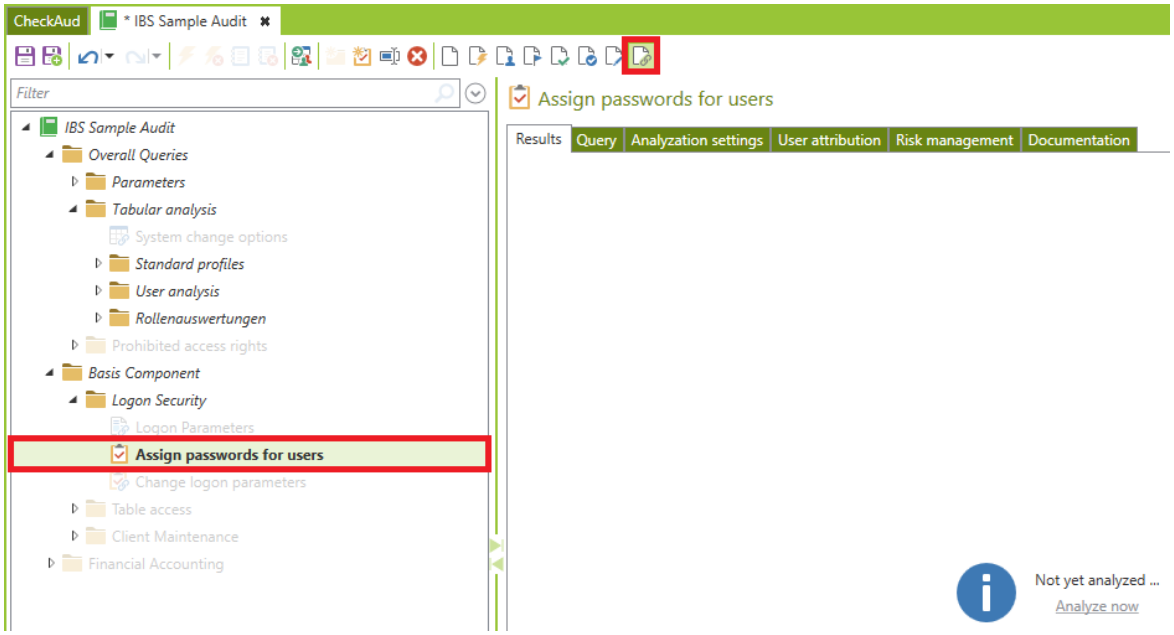



**Abbildung 277 - visualize not referenced elements in the project**

## V - 3.4 Authorization queries (ABAP)

### V - 3.4.1 Create/Changing own queries - graphical view

You can edit the composition of an authorization query on the *Query* tab page:

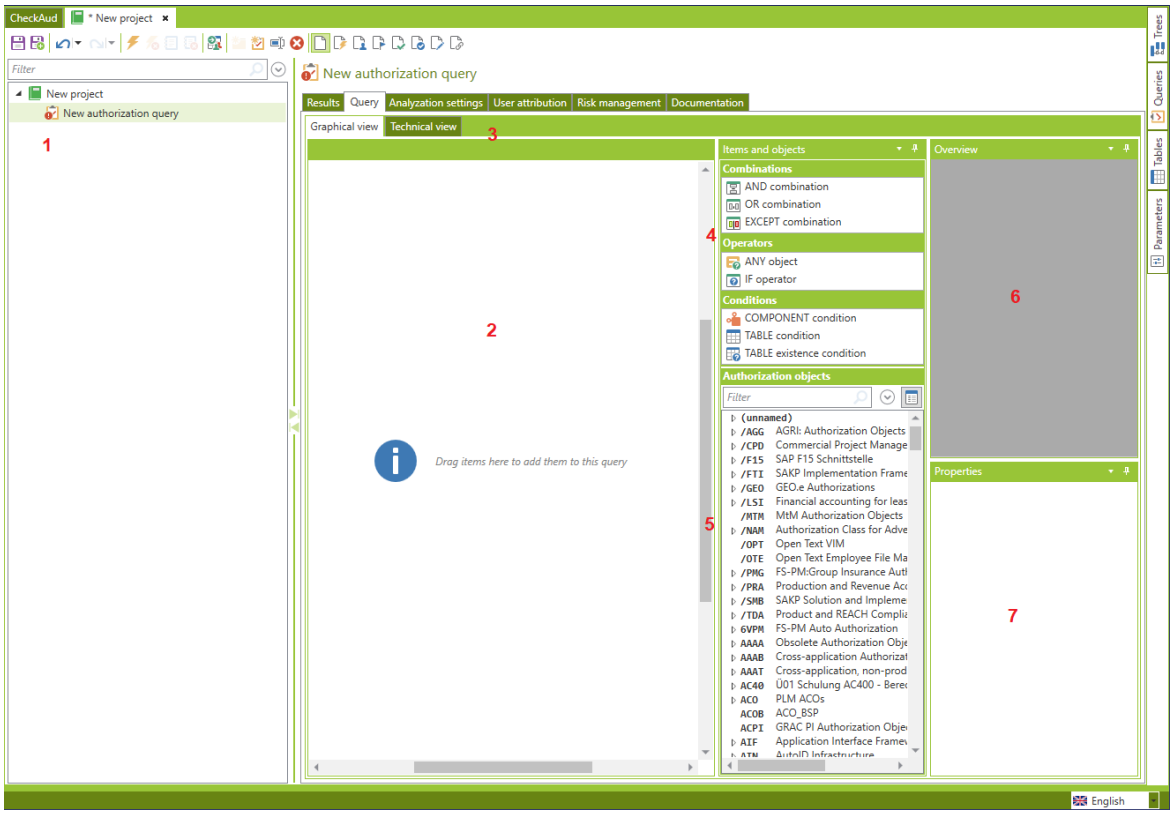



**Figure 278 - Editor for modifying authorization queries (ABAP)**

1. New query in the analysis project
2. Editor area, graphical view of the composition of the authorization
3. Editor area, text view of the composition of the authorization
4. Toolbox for selecting logical connectives, operators and conditions
5. Toolbox for selecting the authorization objects included in the snapshot
6. Overview of the graphical view of authorization compositions
7. Editing box for editing the field values/properties of the authorization object selected in the editor area

**Note:** Authorization queries that you create yourself are not subject to the same update procedure as IBS standard queries. When changes are made in the SAP system that require corresponding updates to the query logic, you must update your created authorization queries yourself!

The graphical editor includes a zoom function. This allows you to zoom in on or out of the requests. The zoom function is controlled using the scroll wheel on the mouse or the touch pad. This feature can be helpful for more complex authorization queries.

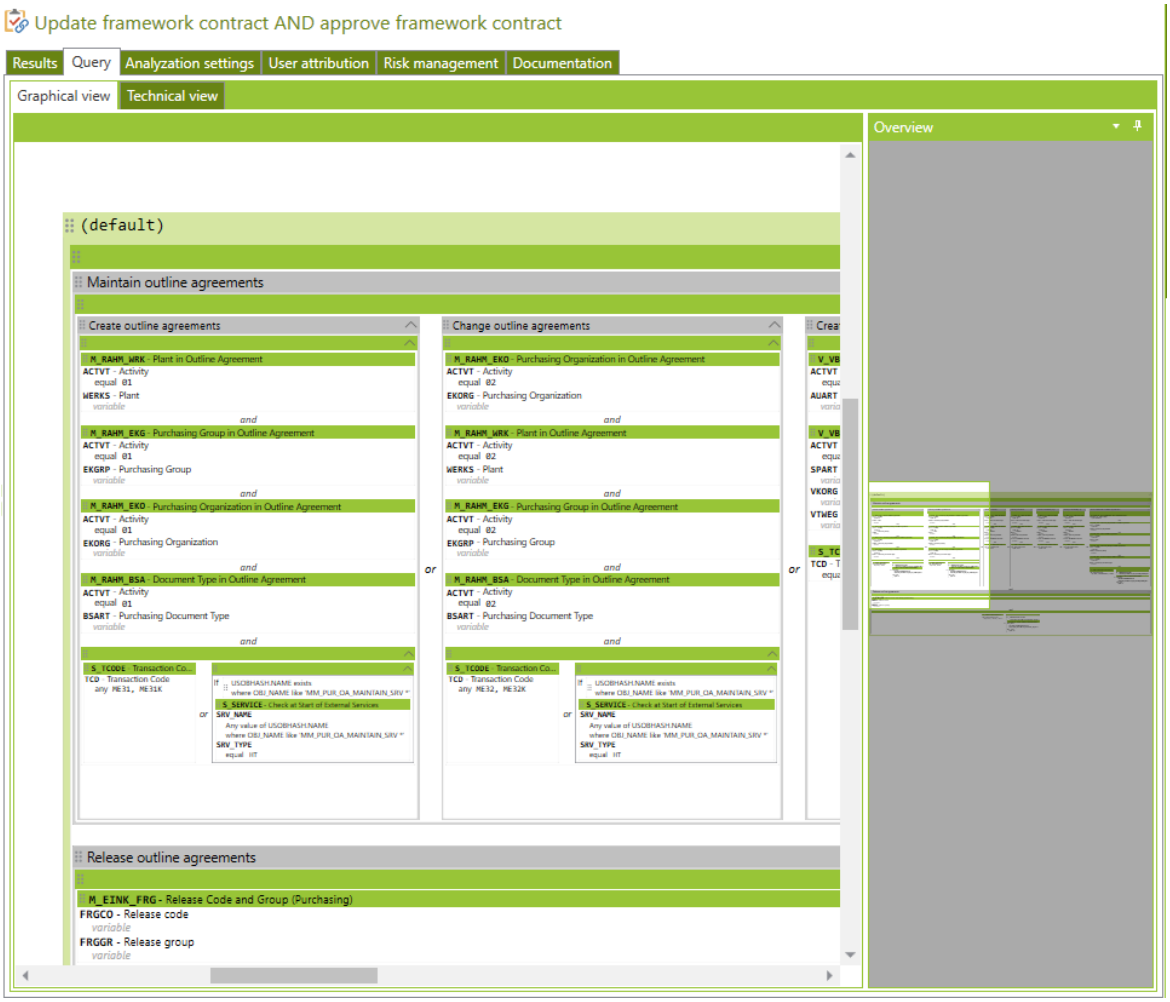



**Figure 279 - Complex query in the graphical editor**

For greater clarity in more complex queries, an overall overview of the query is provided in the graphical editor. The area focused upon in the graphical editor is always the area highlighted in the requests overview.


Figure 280 - Overview window

The whole graphical editor can be operated using drag and drop or the keyboard. A number of different elements are provided for it in the toolbox:


Figure 281 - Toolbox for links, operators and conditions

Boolean operators specify the evaluation logic of authorization objects. For more detailed information about the logical operators for queries, see the chapter *Logical Links for Queries*.

Authorization objects are the building blocks of the authorization query. You can select the object from the relevant toolbox.

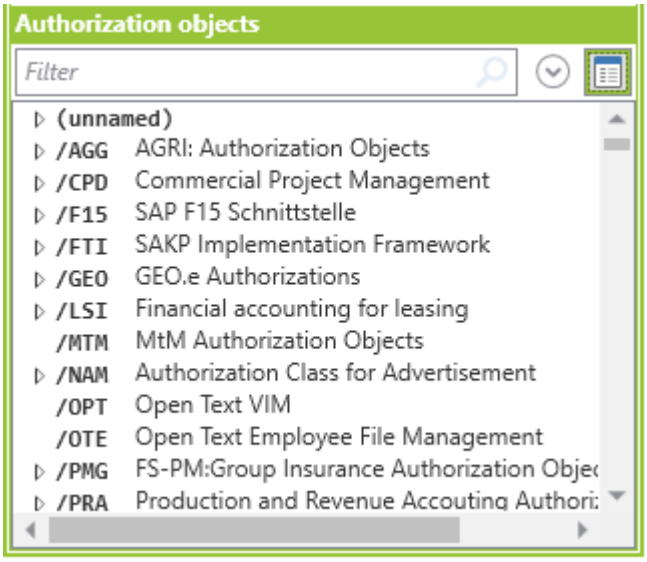



**Figure 282 - Toolbox for available authorization objects**

Since there are a large number of authorization objects, you can use the search function to find specific objects. You can make selections by name, description, class or class description.

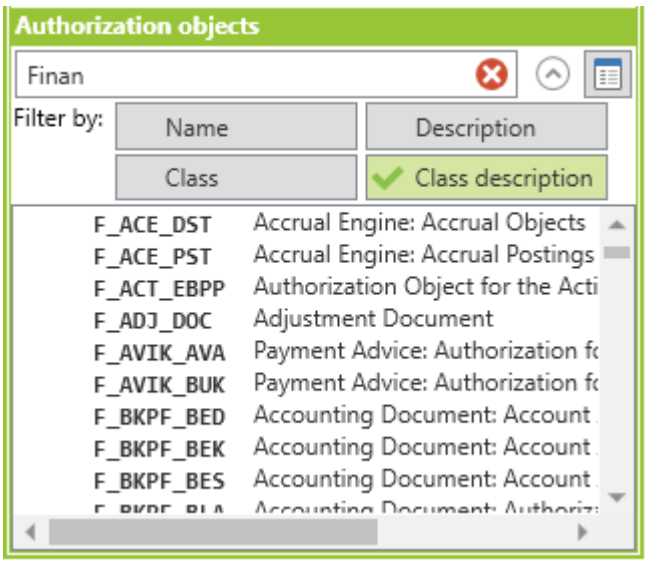



**Figure 283 - Searching for authorization objects**

In addition, you can use the  button for a hierarchical class view of the objects available for selection.

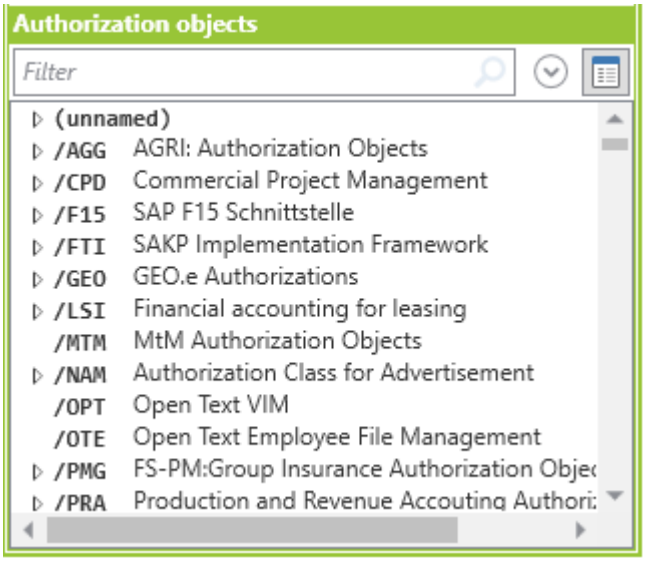



**Figure 284 - Class view of the objects**

Queries that are delivered as standard with CheckAud can also be dragged and dropped directly into the editor for the new authorization query. A personalized query based on the predefined standard queries provided can also be created:

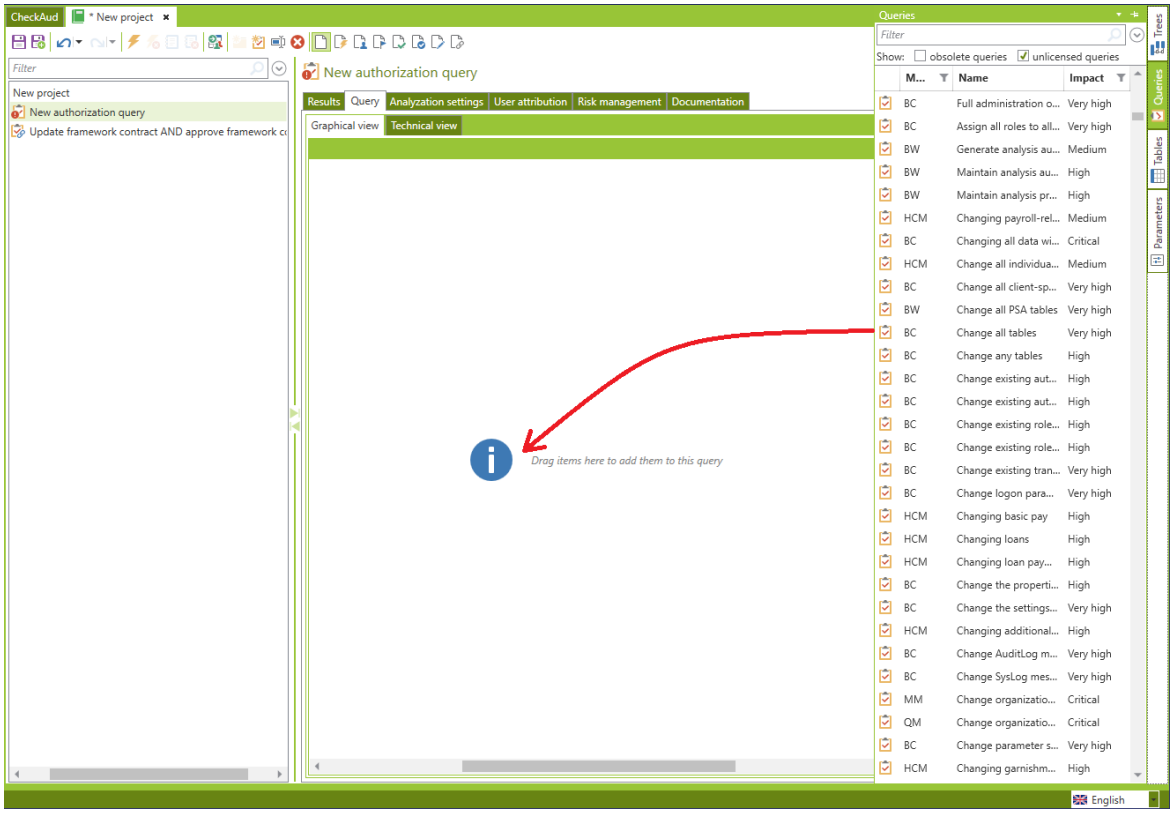



**Figure 285 - Using standard queries in your own queries**

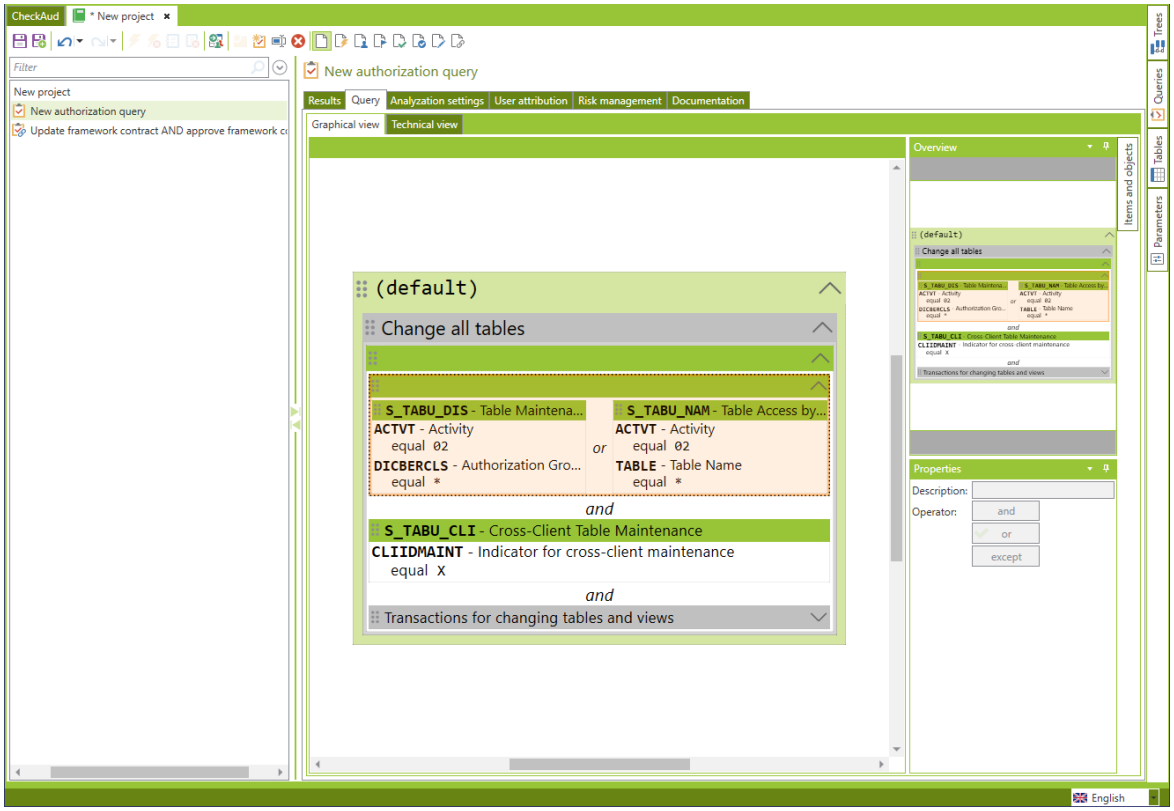



**Figure 286 - Using standard queries in your own queries**

The example below highlights the options available to you while creating authorization queries using the graphical editor. You want to create a query that can be used to check which SAP users are authorized to create vendors in a specific company code.

The following authorization objects are required for this process in the standard SAP system:

F_LFA1_APP
- Defines which activities are permitted for vendor master records
- Field ACTVT Activity 01 (Create)
- Field APPKZ Application authorization F (Financial Accounting)

F_LFA1_BUK
- Defines which activities are permitted in the company code-dependent area of the vendor master record
- Field ACTVT Activity 01 (Create)
- Field BUKRS Company code $ (company code with variable definition)

F_LFA1_GRP
- Defines which activities are permitted for the individual account groups
- Field ACTVT Activity 01 (Create)
- Field KTOKK Account group $ (account group with variable definition)

S_TCODE
- Used to check the authorization for starting the transactions defined within it irrespective of application
- Field TCD, transaction code FK01 or XK01 (standard SAP transactions for creating vendors)

To create the query, you first create an AND operator. The container is initially empty. In the next step, it is filled with the authorization objects for the application level. They are all needed to create vendors in the SAP system, so these authorization objects must be linked by a logical AND.

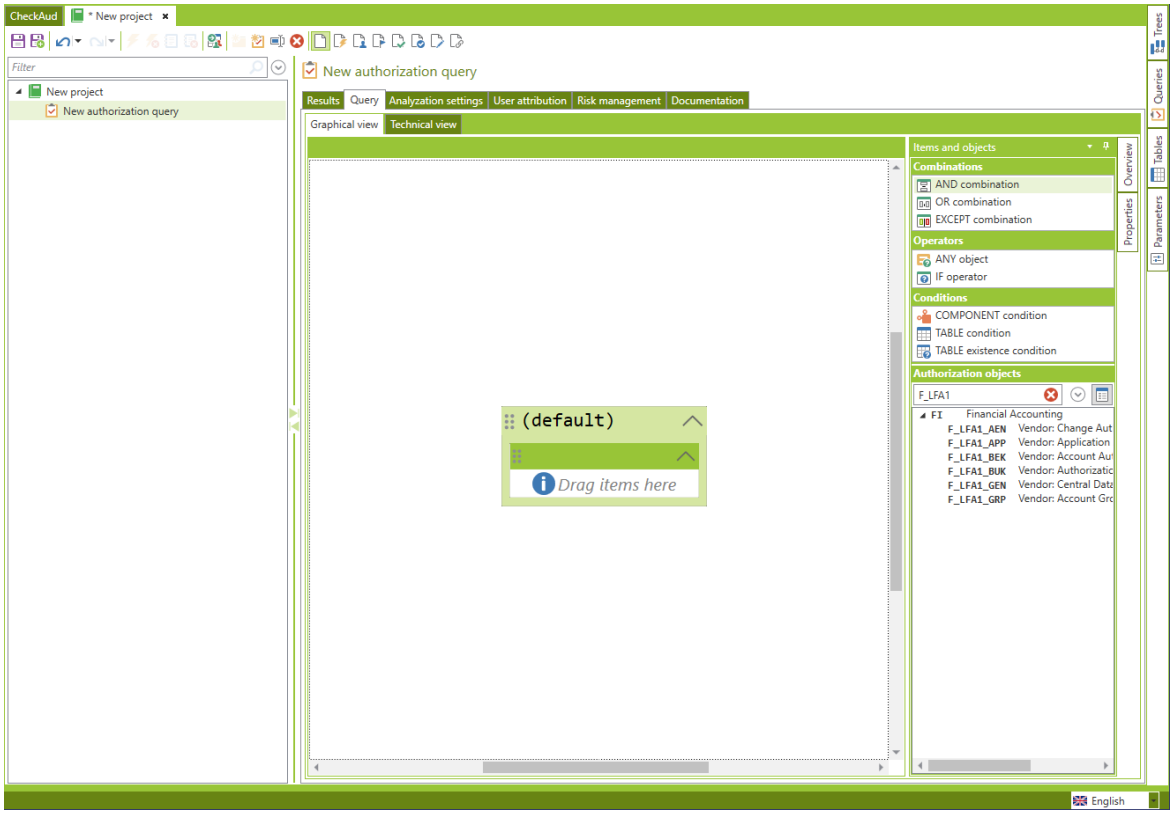



**Figure 287 - Logic container**

To choose the logical operator, drag the appropriate entry from the toolbox. When you right-click the button, a context menu opens. The context menu allows you to expand the request nesting and delete, copy, cut and paste individual elements. Now drag&drop the application authorization objects F_LFA1_APP, F_LFA1_GRP and F_LFA1_BUK into the logical AND container to save them. The objects can be selected from the toolbox via the relevant search options:

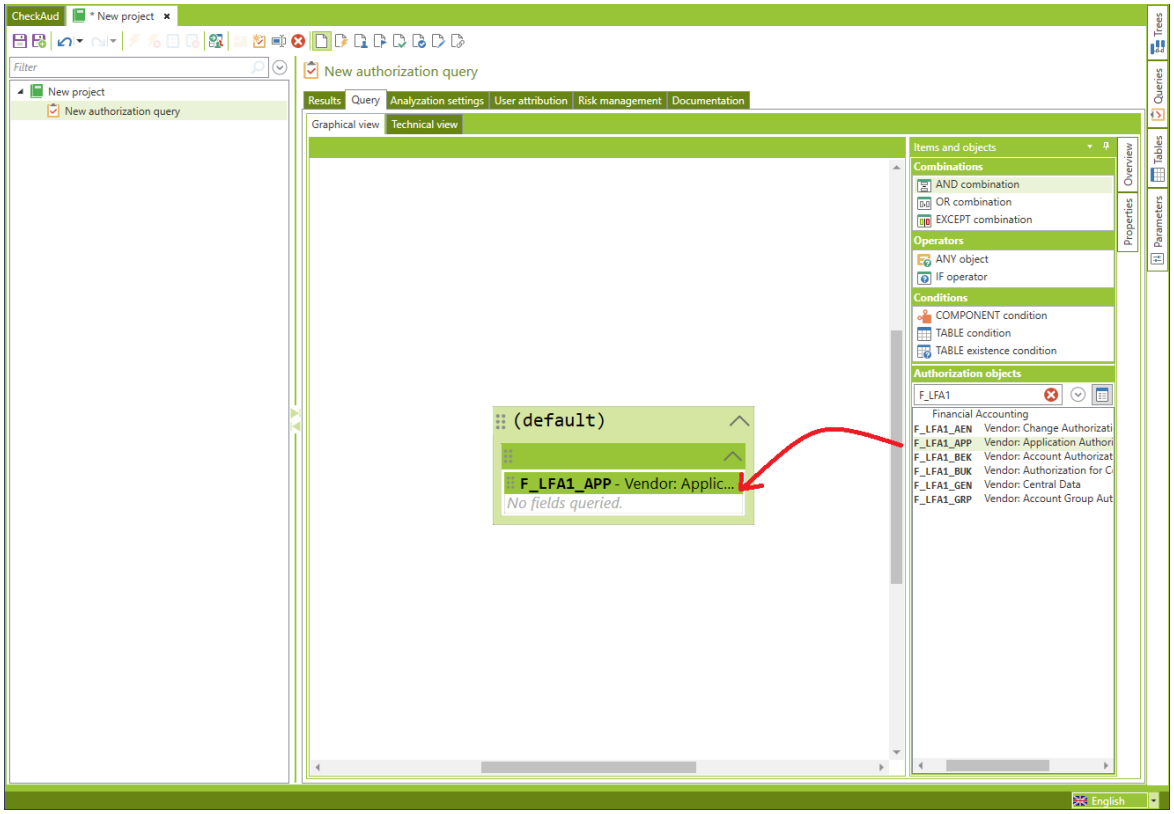



**Figure 288 - Dragging authorization objects to the AND container**

You select the object to edit its properties. You add and then define the request attributes using the  button. As a further alternative, the field value can also be specified as a variable. To do so, click the  button.

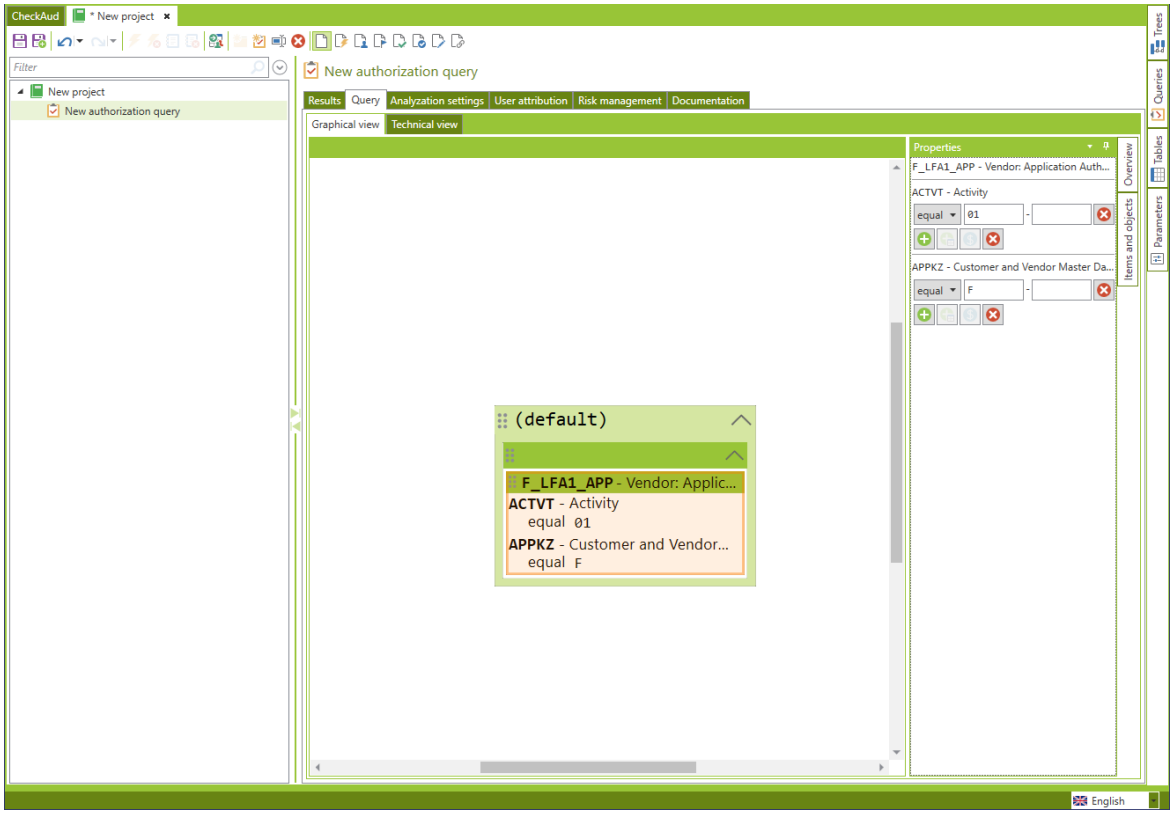



**Figure 289 - Defining the authorization object**

Now repeat this process with the authorization objects F_LFA1_BUK and F_LFA1_GRP that are also required:


**Figure 290 - Selecting additional objects**

The BUKRS field of authorization object F_LFA1_BUK or the KTOKK field of object F_LFA1_GRP are to be defined variably, meaning that they will not receive their final values until before the actual evaluation. This allows a variety of organizations to use the query flexibly without changing the technical composition. To do so, activate the  button for the field value in question.

To complete the query, you must also check the transaction authorization now. There are two standard SAP transactions for creating vendors, FK01 and XK01. The S_TCODE authorization object ensures access to the transactions, which is why it is also required in the query to be created.

In order to ask the question, the query now requires the supplementary information of who owns the S_TCODE authorization object with the transaction FK01 or XK01. In the standard SAP system, however, the field values of an authorization object cannot be linked with the logical OR, which means that if the S_TCODE object is defined with the field values FK01 and XK01, the result will only display users who have access to both transactions. Users who only have access to FK01 or XK01 will not be displayed in this case, even though they are relevant for the result. This is why the S_TCODE authorization object is queried two times – once with the FK01 value and once with the XK01 value. These sub-queries will be integrated with logical OR operators.
This is why in the next step, you drag and drop a new logic container into the query's AND container and define it as an OR container:

The S_TCODE authorization object will now be dragged&dropped into this OR container twice – once with the FK01 value and once with XK01:

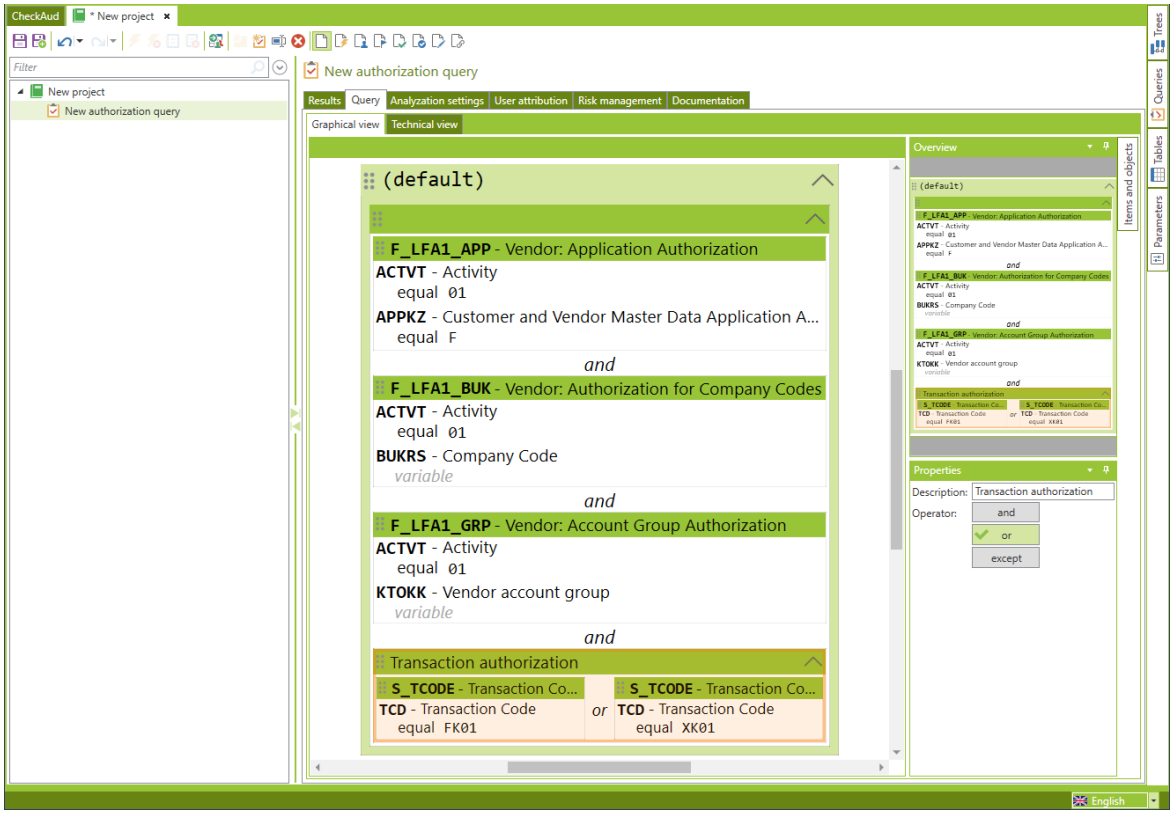



**Figure 291 - Defining S_TCODE**

Now the query is correctly composed and available for evaluation.

Regardless of the fact that field values in the SAP system are only logically linked with AND, CheckAud can also evaluate field value definitions that are logically linked with OR. This is why the S_TCODE query part of the example above can be solved more elegantly, as shown in the following. Instead of evaluating the S_TCODE object twice in the individual OR-linked value, the object is placed in the logical AND container only once. Only the field values are then logically linked with OR.

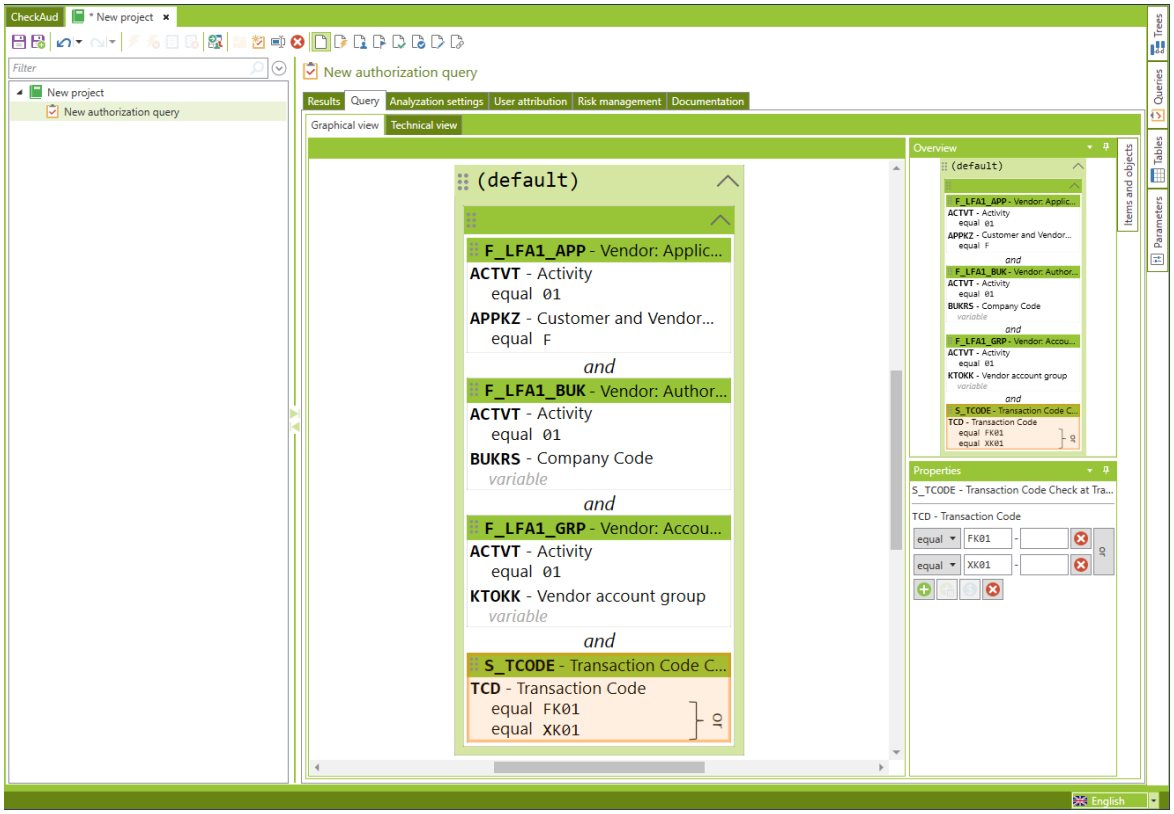



**Figure 292 - Logical OR link at field value level**

You can find a detailed description of the relational operators for field values in the chapter *Relational Operators for Field Values*.

**Note:** when deactivated authorization objects are used in the queries, they will be marked in gray and crossed in the graphical editor. Also these deactivated objects will be grayed out in the authorization origin. A detailled information about the origin by roles or profiles is not available.

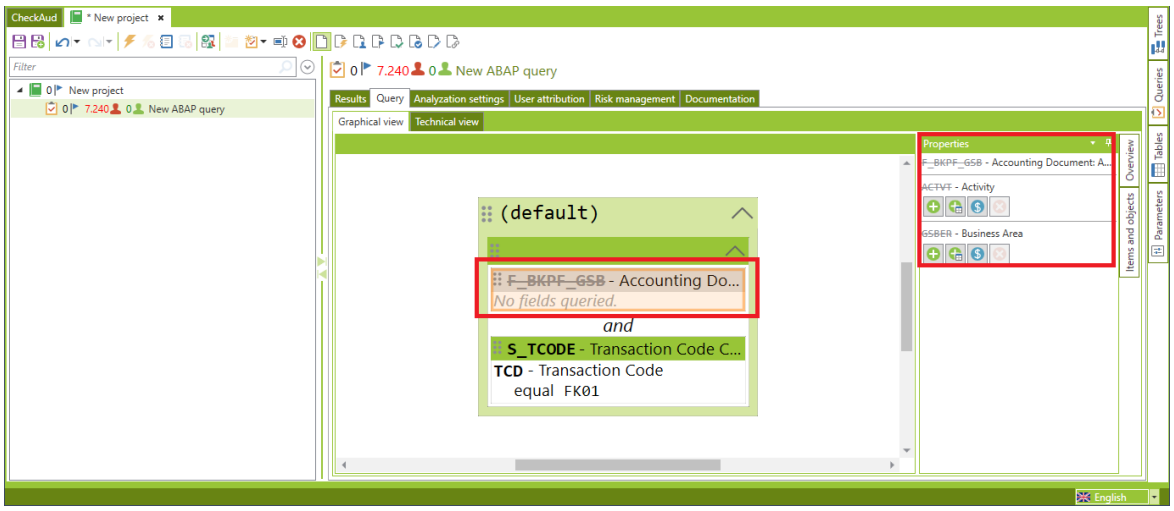



**Figure 293 - Display of deactivated authorization objects**

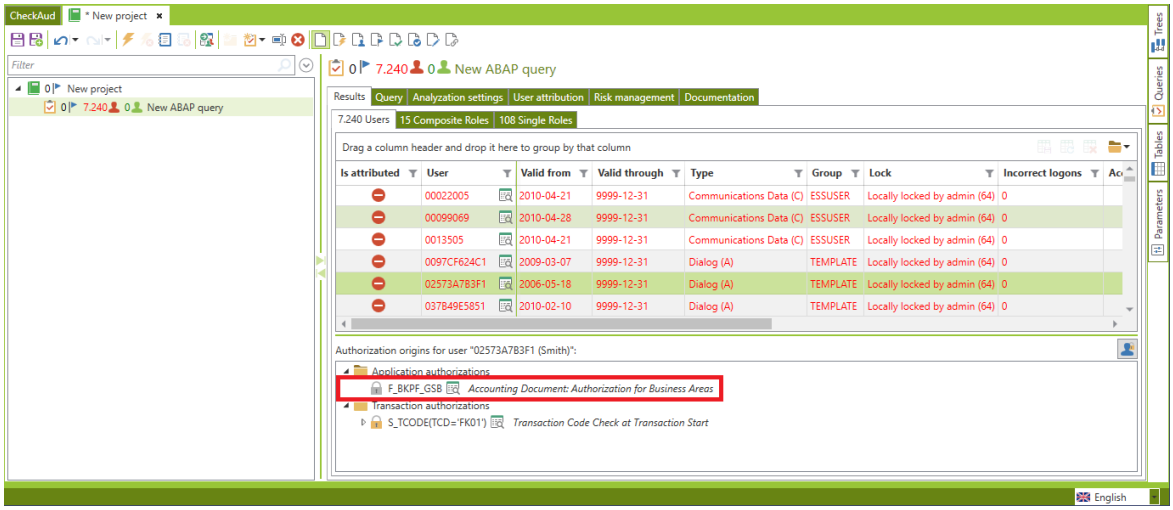



**Figure 294 - Display of deactivated authorization objects**

## V - 3.4.2 Create/Changing own queries - technical view

As an alternative option, the text editor can be used to create authorization queries. To do so, you must switch from the Graphical View to the Technical View.

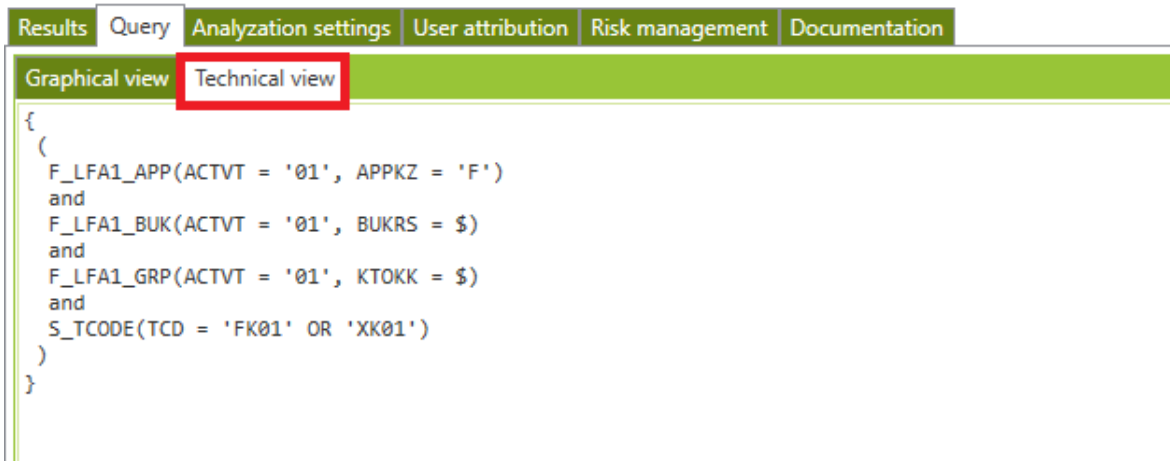



**Figure 295 - technical editor for modifying authorization queries (ABAP)**

The authorization query created in the chapter *Creating/Changing Your Own Queries – Graphical Editor* is textually displayed as follows:

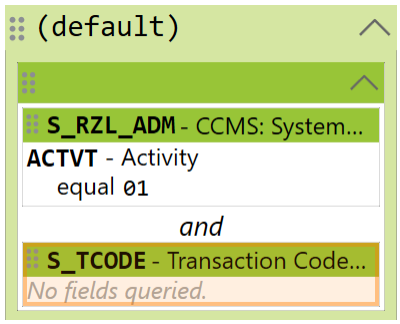
```
{
 (
  'F_LFA1_APP'('ACTVT' = '01', 'APPKZ' = 'F')
  and
  'F_LFA1_BUK'('ACTVT' = '01', 'BUKRS' = $)
  and
  'F_LFA1_GRP'('ACTVT' = '01', 'KTOKK' = $)
  and
```

```
  (
   'S_TCODE'('TCD' = 'FK01' OR 'XK01')
  )
 )
}
```

### V - 3.4.3 Logical connectives for queries

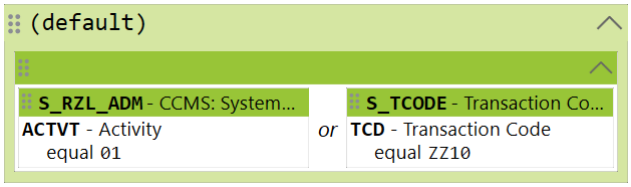
*Logical connectives* are used to link multiple authorization objects to each other. Three types of connectives are available:

AND connective for logical AND, expression is evaluated as true, if both parts of the connective are true



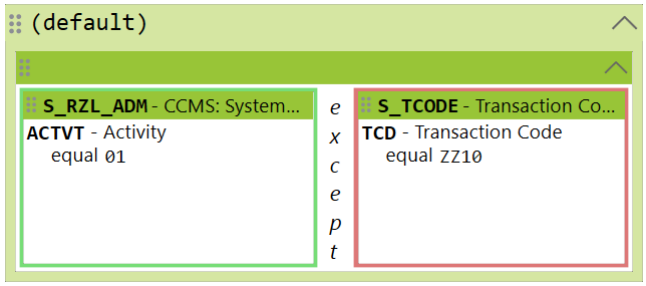

```
{
 (
  S_RZL_ADM(ACTVT = '01')
  and
  S_TCODE()
 )
}
```

OR connective for logical OR, expression is evaluated as true if at least one of the twoe parts of the connective is true




```
{
 (
  S_RZL_ADM(ACTVT = '01')
  or
  S_TCODE(TCD = 'ZZ10')
 )
}
```

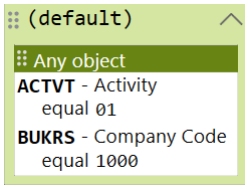
EXCEPT connective for logical EXCEPT, expression ist evaluated as true if one part of the link is true and the other is false




```
{
 (
  S_TCODE(TCD = 'RZ10')
  except
  S_TCODE(TCD = 'ZZ10')
 )
}
```

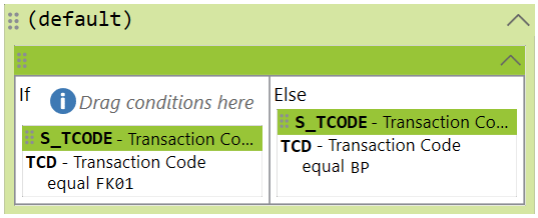
### V - 3.4.4 Logical operators for queries

ANY — Operator for querying specific field values in any object. See the chapter *ANY Operator*




```
{
 ANY(ACTVT = '01', BUKRS = '1000')
}
```

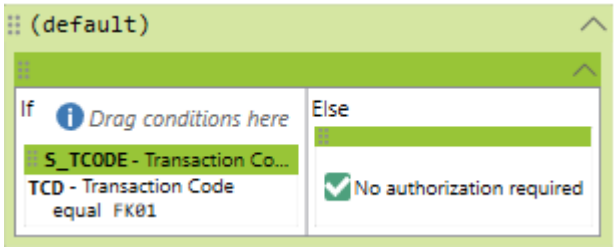
IF — Operator for querying a condition with a subsequent THEN ELSE selection




```
{
 if
 {
  S_TCODE(TCD = 'FK01')
 }
 else
 {
  S_TCODE(TCD = 'BP')
 }
}
```

***Note***: The IF operator can be used only in combination with a defined *condition*; see the chapter below

NO AUTHORIZATION REQUIRED — Operator for query in combination with IF operator, can be used in the THEN / ELSE part when no authorization is required

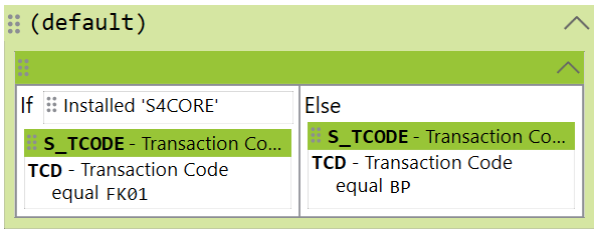



```
{
 if
 {
  S_TCODE(TCD = 'FK01')
 }
 else
 {
  NO_AUTHORIZATION_REQUIRED
 }
}
```

### V - 3.4.5 Conditions for queries

*COMPONENT* condition

Condition for IF operator that enables queries of release or patch levels or whether or not components are installed

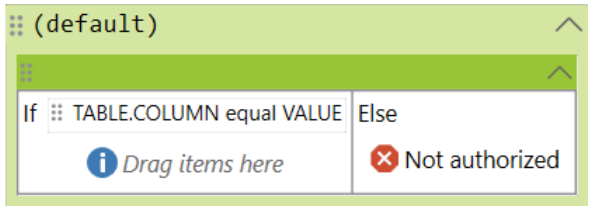



```
{
 if installed(S4CORE)
 {
  S_TCODE(TCD = 'BP')
 }
 else
 {
  S_TCODE(TCD = 'FK01')
 }
}
```

For additional information about using the COMPONENT condition, see the chapter *Release-Independent Authorization Queries*.

*TABLE* condition

Condition for the IF operator that enables queries for specific table entries

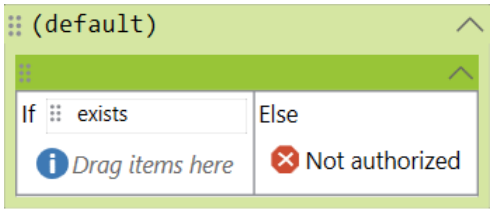



```
{
 if TABLE.COLUMN = 'VALUE'
 {
 }
}
```

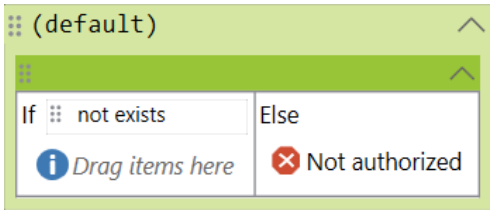
For additional information about using the TABLE condition, see the chapter *Customizing-Dependent Queries*.

*TABLE EXISTENCE condition*

Condition for the IF operator that enables queries to check, if a table exists / not exists in the SAP system




```
{
 if TABELLE EXISTS
 {
 }
}
```

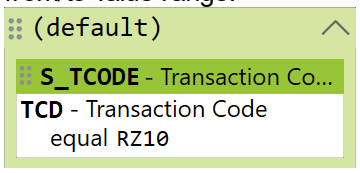



```
{
 if TABELLE NOT EXISTS
 {
 }
}
```

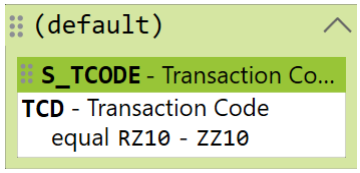
### V - 3.4.6 Relational operators for field values

The fields of an authorization object can be evaluated using relational operators. The following relational operators are available:

EQUAL Expression is evaluated with true if the exact value definition was found. You can enter a from/to value range.

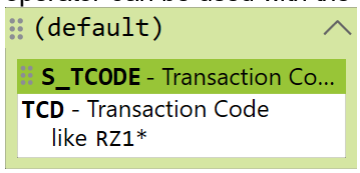



```
{
 S_TCODE(TCD = 'RZ10')
}
```



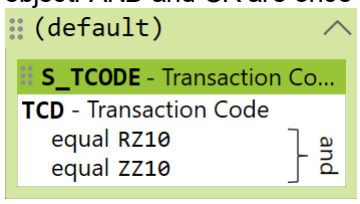

```
{
 S_TCODE(TCD = 'RZ10'-'ZZ10')
}
```

LIKE Expression is evaluated with true if part of the value definition was found. The relational operator can be used with the wildcard * at the end of the string.

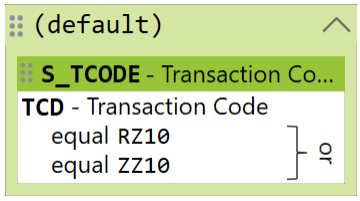



```
{
 S_TCODE(TCD ~ 'RZ1*')
}
```

The EQUAL and LIKE relational operators allow you to logically link multiple field values within the object. AND and OR are once again available here:

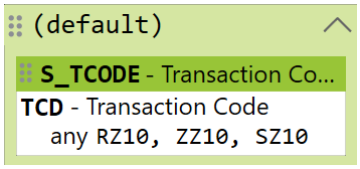



```
{
 S_TCODE(TCD = 'RZ10' AND 'ZZ10')
}
```



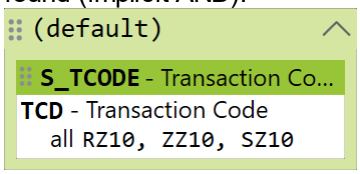

```
{
 S_TCODE(TCD = 'RZ10' OR 'ZZ10')
}
```

ANY Expression is evaluated with true if at least one of the specified field value definitions was found (implicit OR).




```
{
 S_TCODE(TCD ANY ('RZ10', 'ZZ10', 'SZ10'))
}
```

ALL Expression is evaluated with true if all the specified field value definitions were found (implicit AND).




```
{
 S_TCODE(TCD ALL ('RZ10', 'ZZ10', 'SZ10'))
}
```

### V - 3.4.7 ANY object operator

In addition to an authorization object query, CheckAud also provides the option of querying authorization values at field level, independently of the authorization object. This could be required for the following questions, for example:

Which users have access to a specific company code?
Which users have change rights at a specific plant?

Such questions relate to general access at the organizational level rather than a query of specific functions. You can use the ANY operator to map such questions. It is used instead of an authorization object.


**Figure 296 - Adding the ANY operator to the authorization query**

By selecting the *Any object* checkbox in the request, you can edit the properties of the ANY query (by adding field values).

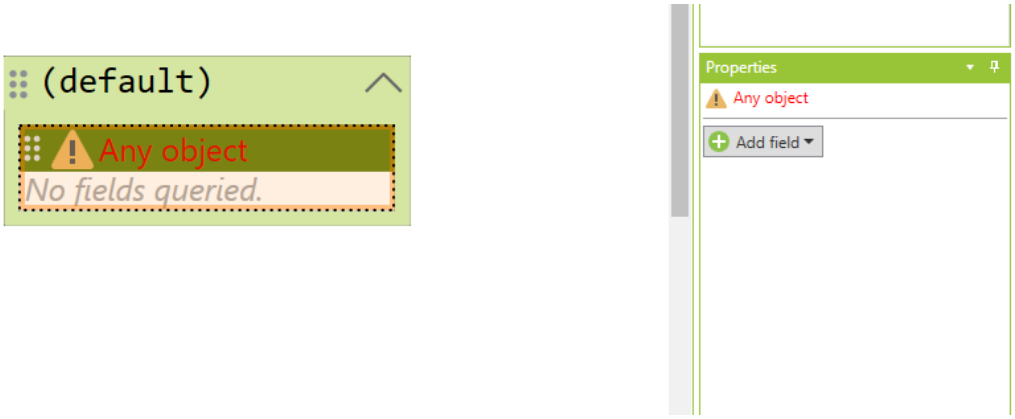



**Figure 297 - Field definition for the ANY operator**

The Add field button lets you add field values in the ANY operator. In this example, the company code is added. Left-click the desired attributes to select the fields. You can select one or more fields here.

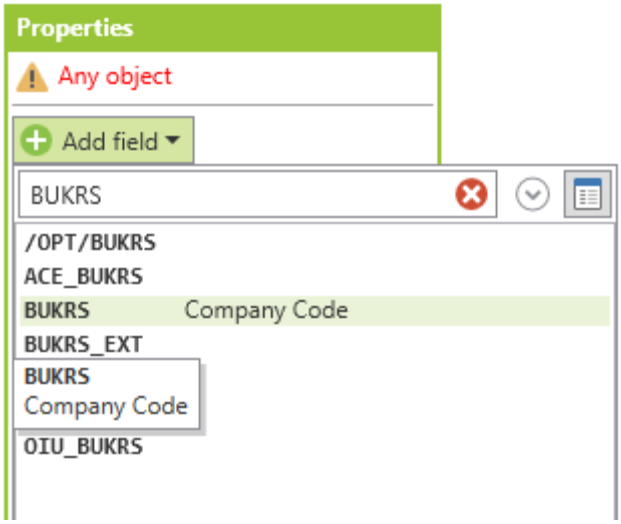



**Figure 298 - Field definition with BUKRS**

Then, click Add selected fields to add the field value to the request. You can add additional fields to the query using the button and then specify their attributes.

Examples:

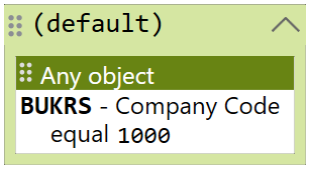



**Figure 299 - ANY operator for searching for objects with BUKRS=1000**

Search for all authorization objects with the field BUKRS (“Company Code”) and display all users with authorization for the company code 1000.

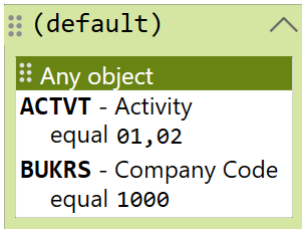



**Figure 300 - ANY operator for searching for objects with BUKRS=1000 and ACTVT=01, 02**

Search for all authorization objects with the fields ACTVT (“Activity”) and BUKRS (“Company Code”) and display all users with create (activity 01) or change (activity 02) authorization for the company code 1000.

In a query, the system handles the ANY operator as an authorization object. You can use it multiple times in one query in any required AND/OR combinations. It can also be combined with other authorization objects and queries.

## V - 3.4.8 Release-independent authorization queries

### Introduction

An SAP system consists of various software components. Each component has a release and a patch level. Patches are issued either to fix errors or to roll out new features. Components installed in an SAP system, including their release and patch levels, are stored in the table CVERS. This table is read out as part of the AUTH table set. The authorizations may vary with the release and patch levels of the individual components. Thus patch rollouts may contain new transactions or authorization objects that must be observed in authorization queries. In order to ensure that the authorizations are correctly evaluated with CheckAud, regardless of differences in the release and patch levels, these levels are retrieved in authorization queries. This is visible in the queries in the IF operator. The following query retrieves both the release level (1) and the patch level (2).

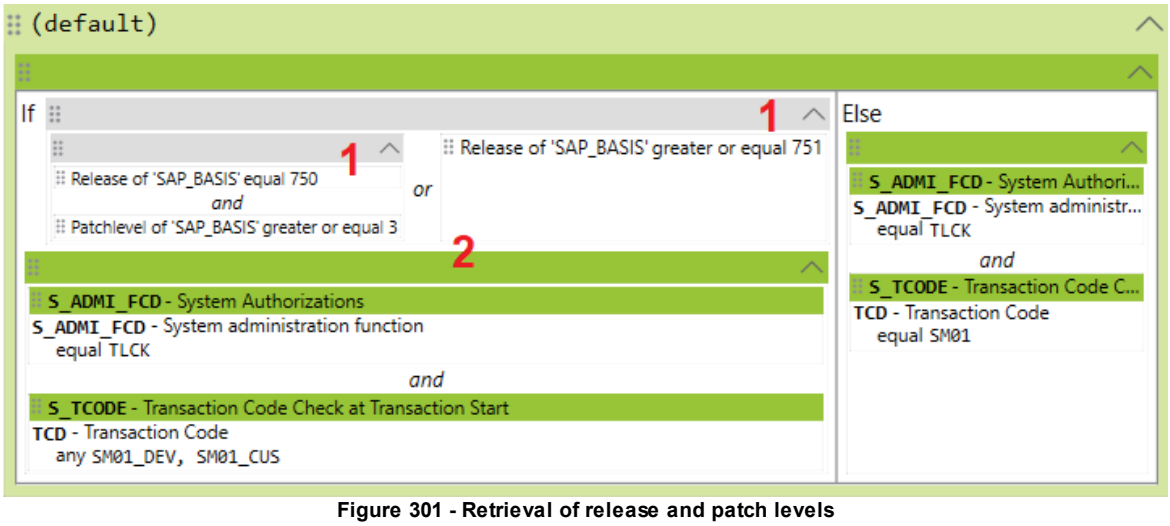



**Figure 301 - Retrieval of release and patch levels**

This system can also query whether particular components are installed in the system. This is of particular relevance when changing to SAP S/4HANA. An S/4HANA system may be identified by the presence of the component S4CORE. The Simplification List for SAP S/4HANA is implemented in

the CheckAud queries. This list contains the changes from SAP ERP to SAP S/4HANA. These differences are represented in queries by querying the S4CORE component.

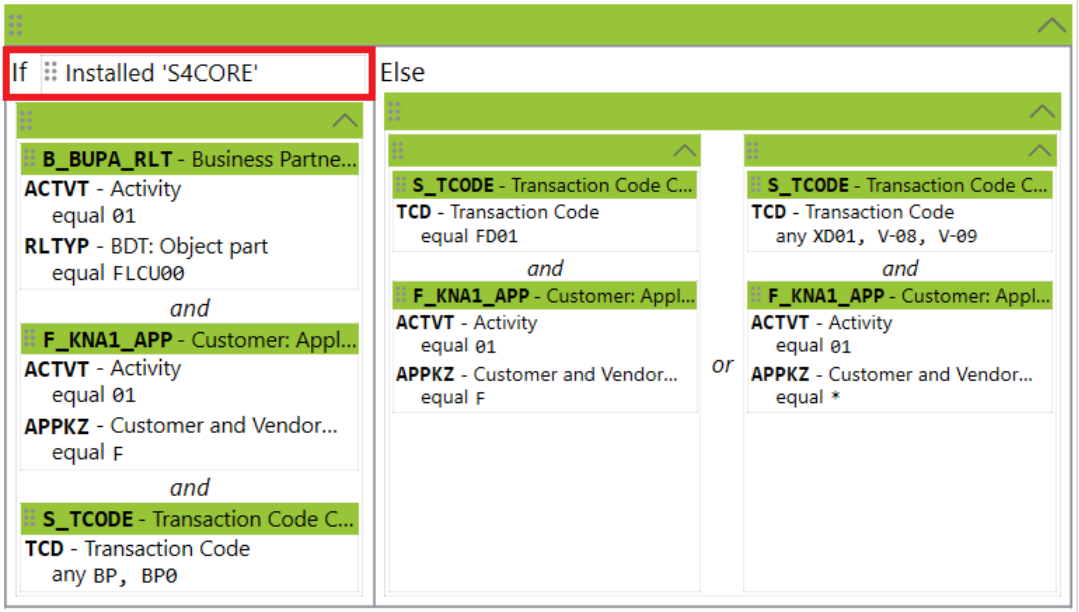



**Figure 302 - Component query**

### Technical implementation

Release independence is implemented in the authorization queries by means of the newly implemented IF operator (1) and the COMPONENT condition (2). These can be found in the design view of an authorization query under Elements and Objects.

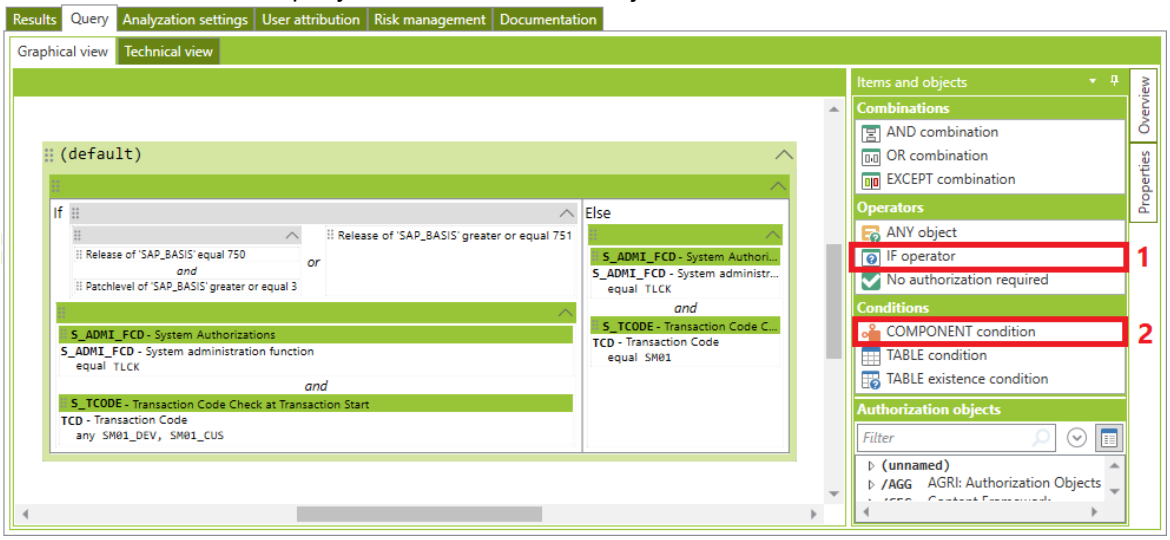



Figure 303 - IF operator and COMPONENT condition

The IF operator may be used at any point in the query. This is dependent on where the differences in the components or release levels affect the queries. Figure 303 shows an IF query at the top level of a query. This is useful when the queries for different release levels differ overall. In figure

304, the IF query is integrated into the authorization query, because the three authorization objects F_KNA1_BUK, F_KNA1_GEN and F_KNA1_GRP are identical regardless of release level.

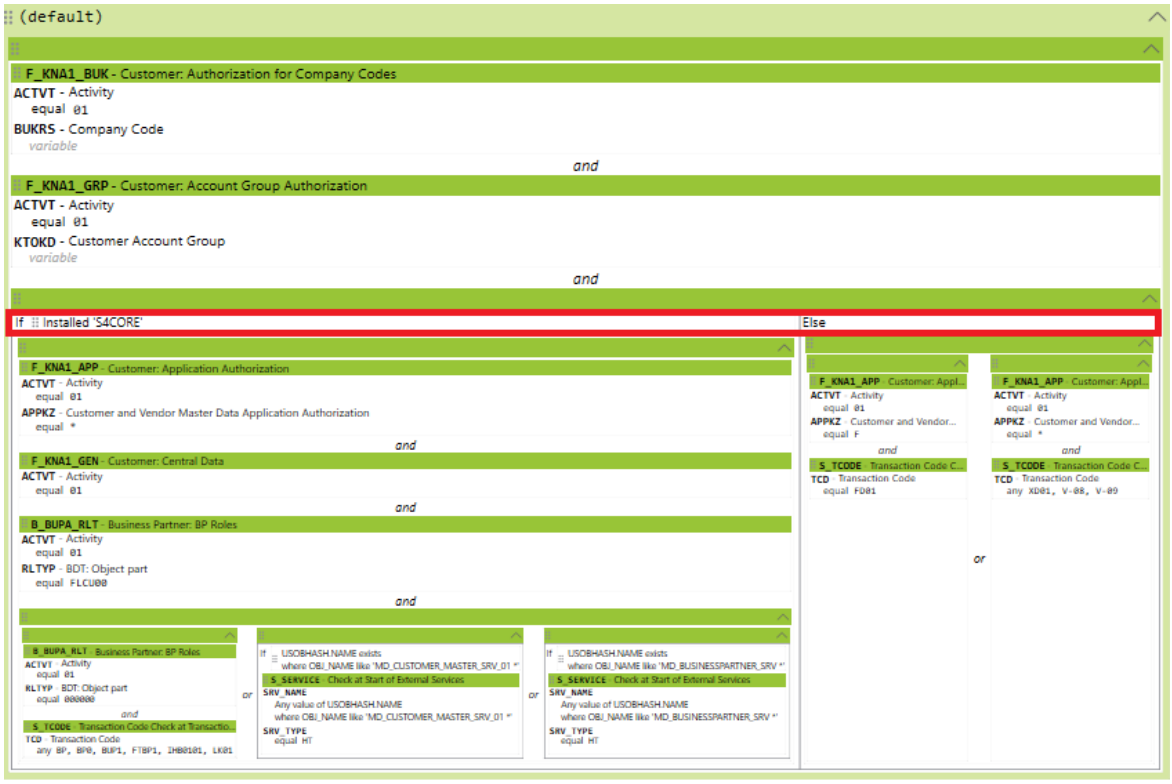



Figure 305 - IF operator in a query

### Structure of a release-independent authorization query - Graphical view

To retrieve the release or patch level from the design view of an authorization query, drag the IF operator into the editing area (step 1 in figure 306). Next, drag the COMPONENT condition into the area marked *Drag conditions here* (step 2 in figure 306)

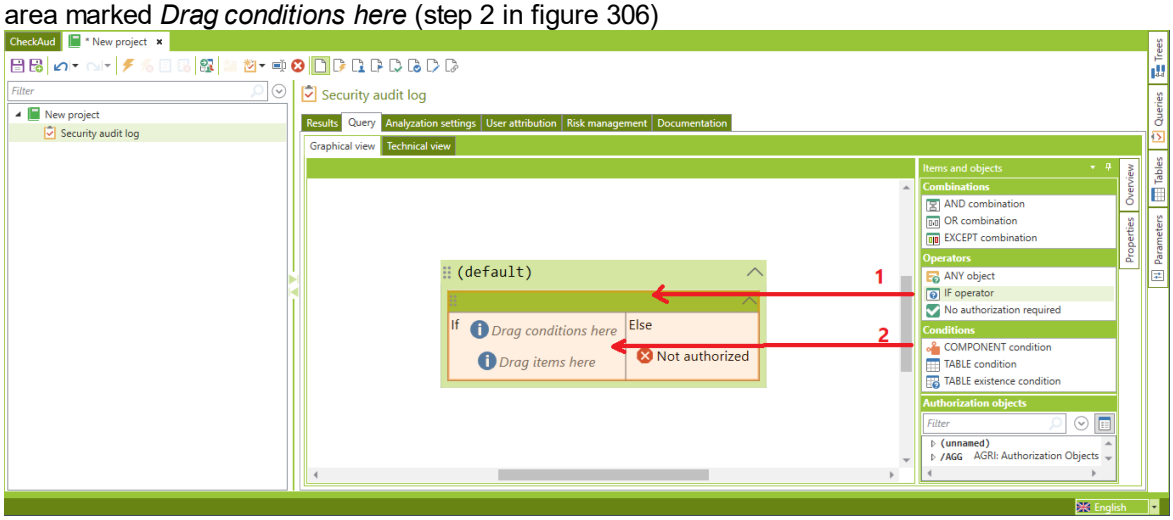



**Figure 306 - Inserting the IF operator in a query**

By default, the value displayed in the IF operator is "Release of  equal". Click this entry to change the value in the Properties area. Complete the following fields in this area:

**Component operator**

Select the type of component to be queried here:

| | |
|---|---|
| *Release of* | Select this to query the release level of a component. |
| *Patch level of* | Select this to query the patch level of a component. |
| *Installed* | Select this to query whether a particular component is installed. |
| *Not installed* | Select this to query whether a particular component is not installed. |

**Components**

Select the component to be queried here. For suggestions to be shown here, a snapshot must have been selected previously. The components of the snapshot are then suggested as values (from the table CVERS).

**Relational operators**

For the component operators *Release of* and *Patch level of*, select the comparison operator here:
Less than
Less than or equal to
Equal
Like
Not equal to
Unlike
Greater than or equal to
Greater than

**Value**

Enter the value for the comparison operator. In the example shown in 307 , the release level of the component SAP_BASIS is queried (greater than or equal to 750).

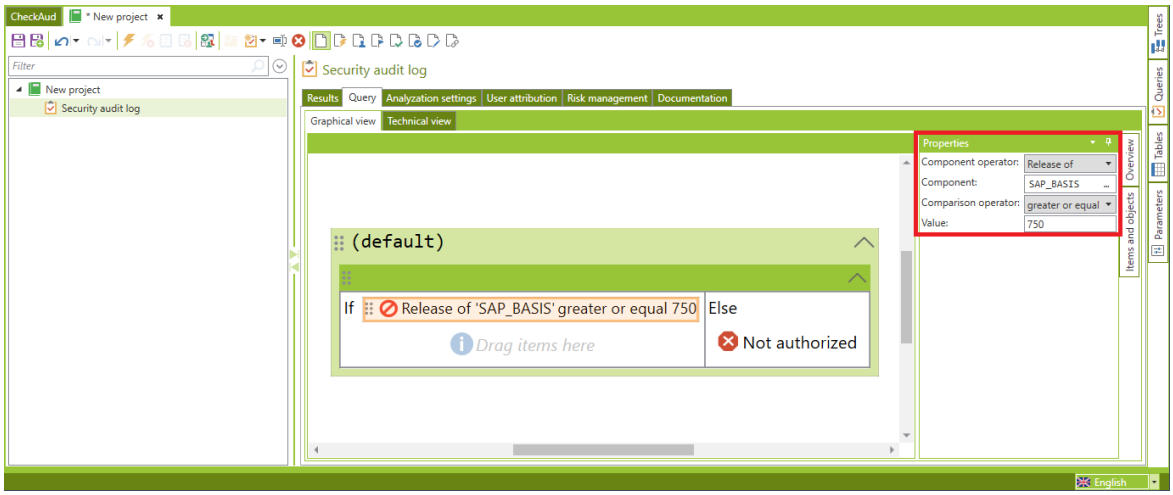



**Figure 307 - Selecting the relational operator**

Component queries may be nested. For example, in order to query a release level and then query the patch level of that release, two queries are required:

1. Query of the release level
2. Query of the patch level of the release

For this purpose, you can drag the IF operator to the *Drag items here* area in both the IF and ELSE areas. Figure 308 shows an example of querying the release level (greater than or equal to 750) and the patch level of that release (greater than or equal to 3). After the components have been queried, update the authorization objects in the query as described in the chapter *Authorization Queries*.

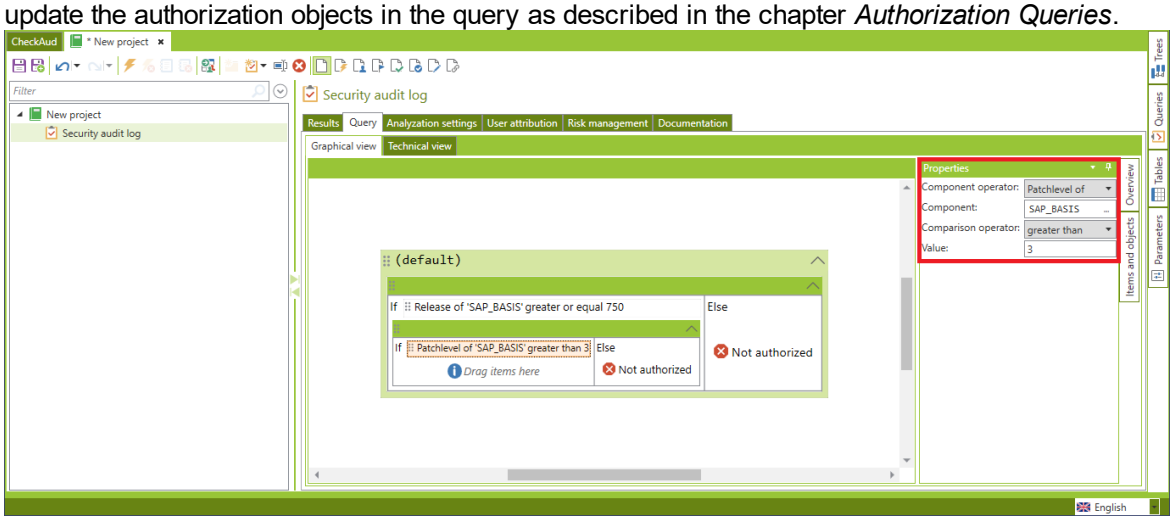



**Figure 308 - Nested IF operators**

### Structure of a release-independent authorization query - Technical view

The technical view represents component queries as follows:

```
if
   <Komponenten-Operator>(<Komponente>) <Vergleichs-Operator> <Wert>
 {
  …
 }
 else
 {
  …
 }
```

### Examples

Querying the release level of the component SAP_BASIS >= 750

```
if
   release(SAP_BASIS) >= 750
```

Querying the release level of the component SAP_BASIS = 750 und Patch-Stand >= 3

```
if
   release(SAP_BASIS) = 750
 {
```

```
if
  patchlevel(SAP_BASIS) >= 3
```

Query whether system is an S/4HANA system (component S4CORE present)

```
if
   installed(S4CORE)
```

Query whether system is not an S/4HANA system

```
if
   not installed(S4CORE)
```

### Displaying with selected snapshot

If you have selected a snapshot in the analysis project, then the current evaluation path is shown in the graphical query view for querying release levels. The part that is not evaluated is translucent. Figure 309 shows a query of the following release level:

```
Release SAP_BASIS = 750 and Patch-Level >= 3
or
Release SAP_BASIS >= 751
```

In the selected snapshot, the component SAP_BASIS has release level 751.

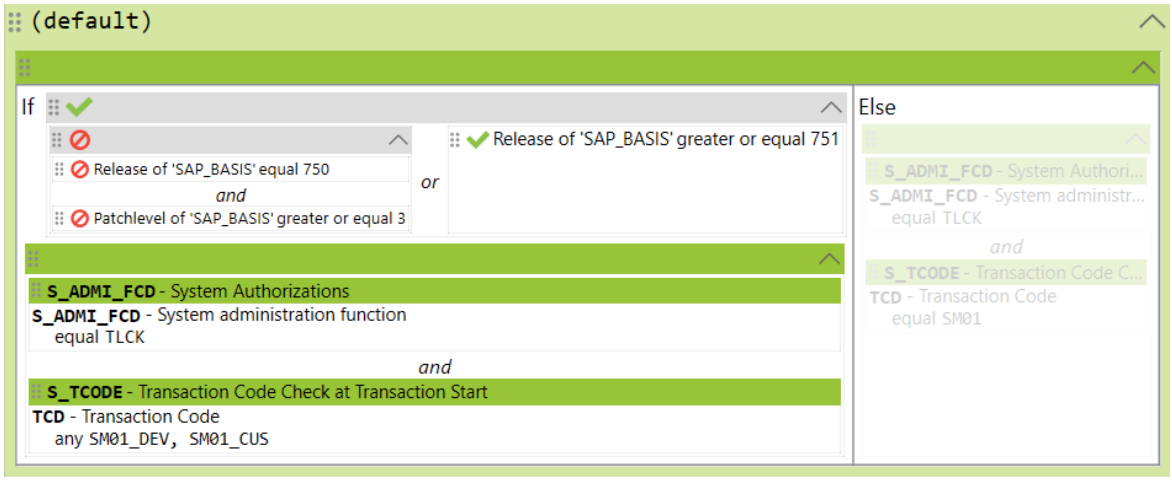



**Figure 309 - IF condition positive**

When a condition is satisfied, then it is shown with a green check mark (here: the part release level SAP_BASIS >= 751). Since the IF part is true, it would be analyzed. Thus the ELSE part of the query is shown translucent. Figure 310 shows the same query with a snapshot in which the component SAP_BASIS has release level 740. Here the IF query is not satisfied, so the ELSE part is queried. Thus the IF part of the query is shown translucent.

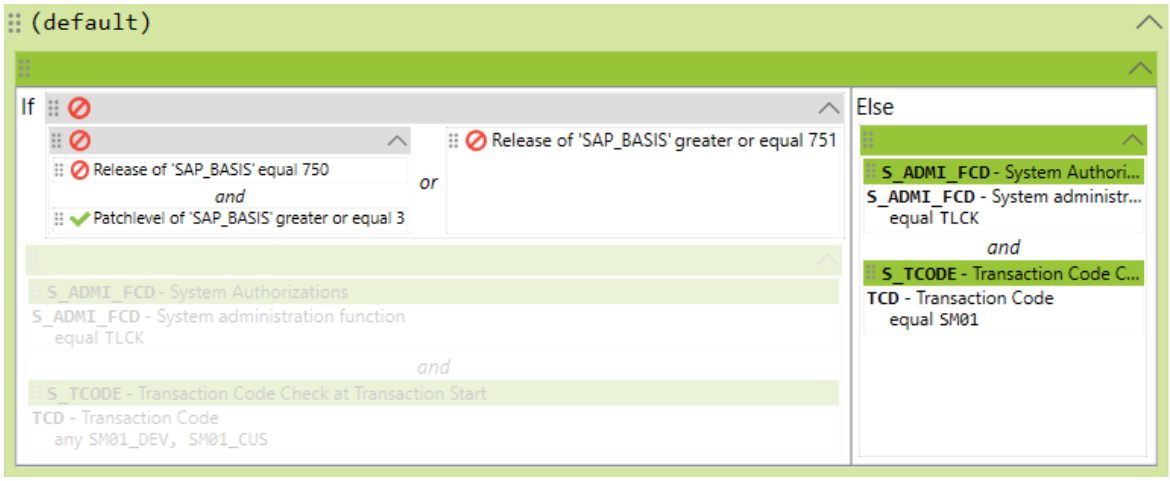



**Figure 310 - IF condition not positive**

### Examples of use

Below are two examples from the CheckAud standard queries that illustrate the system of release independence.

**Example 1:** New transactions for locking transactions

The system for client-specific locking of transactions was introduced in SAP_BASIS release (or also NetWeaver release) 7.50, patch level 3. Up until then, transactions could be locked only system-wide using transaction SM01. As of this release, transaction SM01 is no longer supported. Instead, the following transactions were introduced:

| | |
|---|---|
| SM01_DEV | System-wide lock on transactions |
| SM01_CUS | Client-specific lock on transactions |

For this query to be evaluated with the correct result, the following query was included here:

```
if
   ((release(SAP_BASIS) = 750 AND patchlevel(SAP_BASIS) >= 3) OR
release(SAP_BASIS) >= 751)
```

In Figure 311 the transactions SM01_DEV and SM01_CUS are evaluated if the release level = 750 and patch level >= 3 or the release level >= 751. In all other cases, transaction SM01 is evaluated.

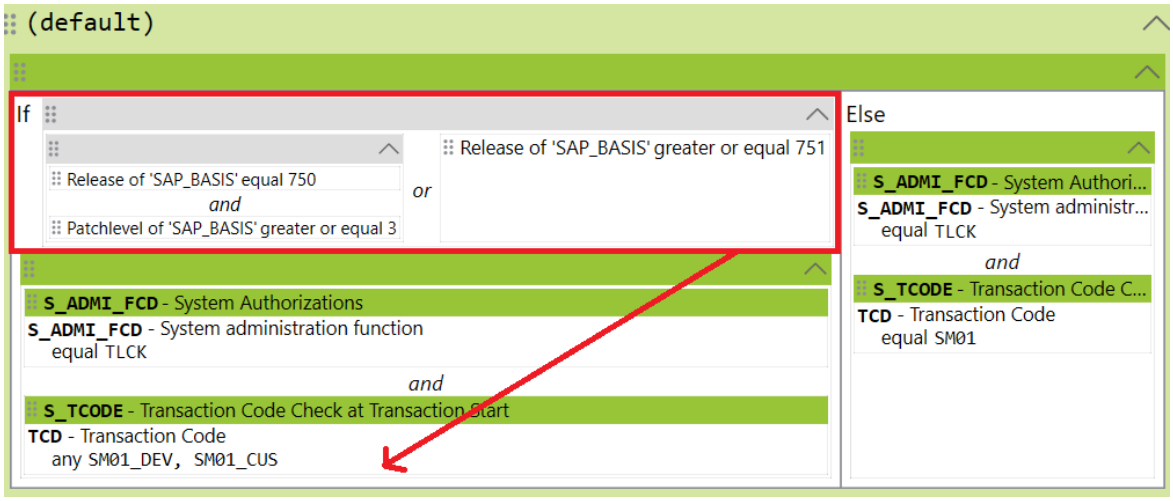



**Figure 311 - Authorization to lock transactions**

**Example 2:** Differing transactions in SAP S/4HANA for customer maintenance

Some of the transactions used in SAP S/4HANA differ from those in SAP ERP. These changes are described in the Simplification List for SAP S/4HANA. For example, the transactions FD* / VD* / XD* are no longer used to maintain customers. Due to the Business Partner Approach in SAP S/4HANA, customers are Business Partners (GP role FLCU00). Thus the transaction GP is used to maintain customers. For this reason, queries for customer maintenance query in CheckAud whether the system is an S/4HANA system (Figure 312):

```
if
  installed(S4CORE)
```

If the system is an S/4HANA system, the object F_BUPA_RLT and the transactions BP and BP0 are queried in addition to the object F_KNA1_APP. If the system is not an S/4HANA system, then the transactions are queried without the business partner object F_BUPA_RLT. (Figure 312)

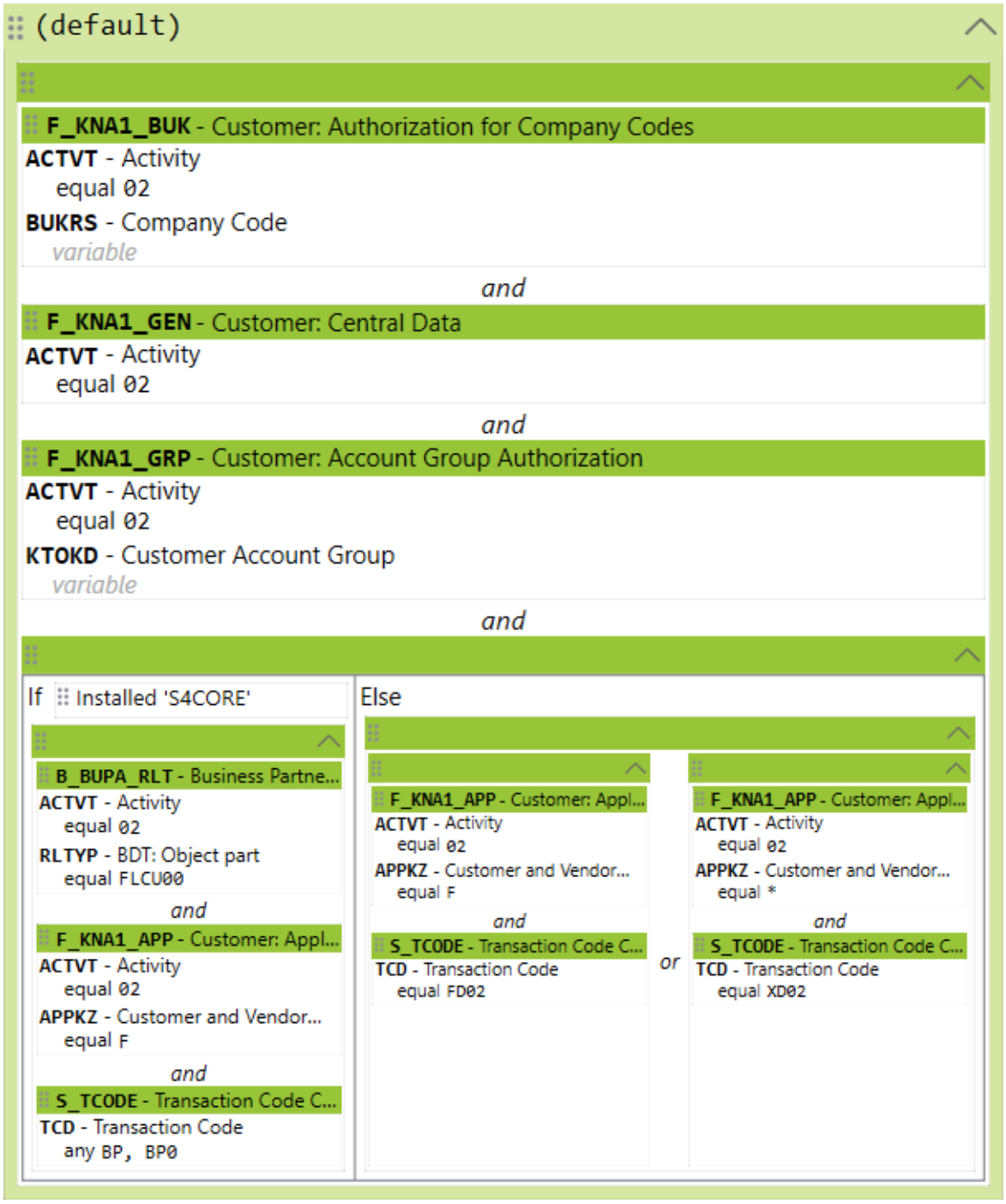



**Figure 312 - Authorization to create customers**

### V - 3.4.9 Customizing-dependent queries

### Introduction

The SAP system allows you to configure certain functions using table entries. For example, the PRGN_CUST and USR_CUST tables contain Customizing settings for the user/authorization system. The settings selected have different effects on authorization queries in CheckAud. The corresponding tables are read out using the AUTH table set.

One example is the optional S_USER_SAS authorization object in authorization management. The PRGN_CUST table contains a switch (CHECK_S_USER_SAS) for controlling this object. Customizing-dependent queries allow you to determine the selected Customizing switch in an authorization evaluation and evaluate the authorization query against it. The Customizing-dependent query is shown in (1) (figure 313) Note that the S_USER_SAS authorization object is only activated by default for NetWeaver Release 7.31 or higher. For more information about creating release-independent queries, refer to the chapter *Release-Independent Authorization* Queries.

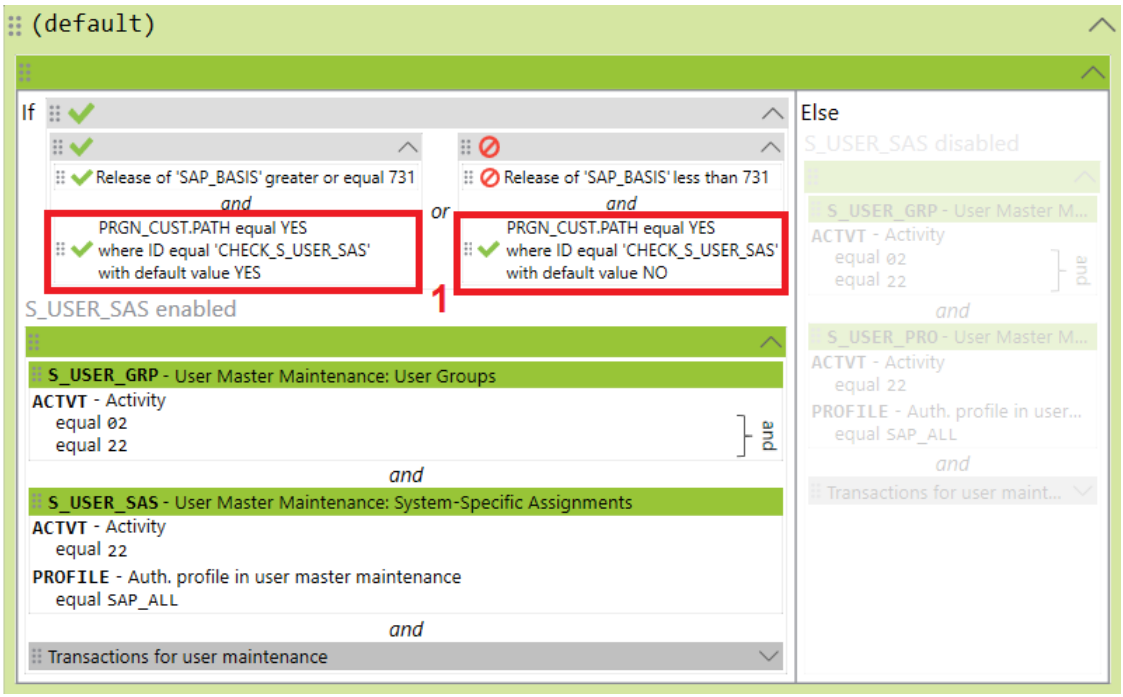



**Figure 313 - Customizing-dependent authorization in queries**

### Structure of a Customizing-dependent - Graphical view

To create a Customizing-dependent query, drag the IF operator to the editing area in the design view of the authorization query (step 1 in figure 314) You then drag the table condition to the *Drag conditions here* area (step 2 in figure 314).

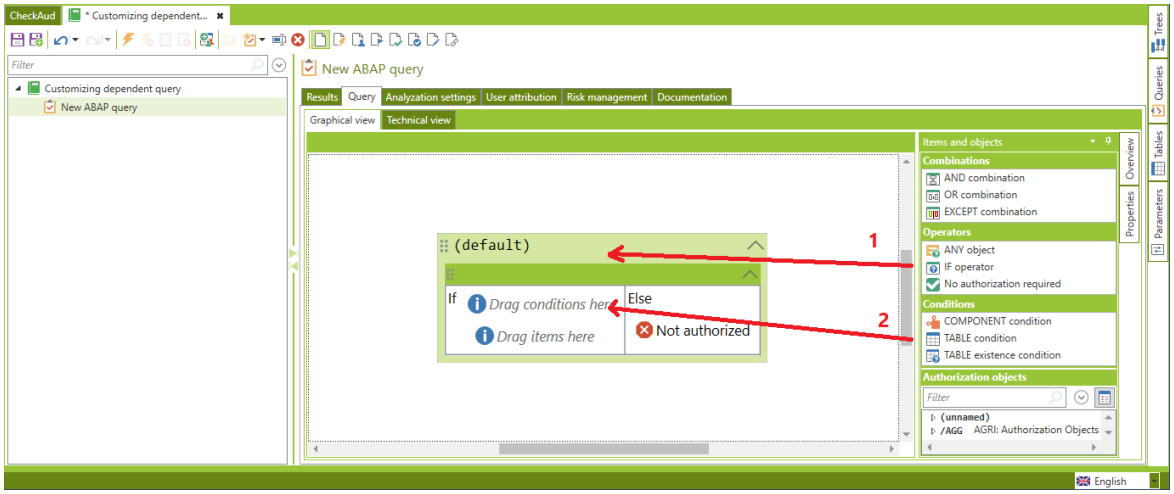



**Figure 314 - Inserting the IF operator in a query**

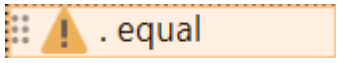
The value  is displayed by default in the IF parameter. Click this entry to edit the corresponding values in the *Properties* area (figure 315).


**Figure 315 - TABLE condition properties**

Complete the following fields in this area:

**Table**

Select the table in which the specific Customizing switches have been defined. Select a snapshot first to have suitable suggestions displayed here. All the tables included in the snapshot are then displayed.

**Column**

This field displays the columns contained in the table selected in the previous step. Select the column that contains the Customizing switch attribute.

**Relational operator**

Select one of the following relational operator options:

Less than
Less than or equal to
Equal
Like
Not equal to
Unlike
Greater than or equal to
Greater than
Is null
Is not null
Exists
not exist

**Comparison value**

Enter the value for the comparison operator. This value is the criterion that must be fulfilled under the selected column, while taking the subsequent Where condition into account.

**Default value**

Select this checkbox to apply a specified default value. This default value is applied in the following situations:

a. The Where condition identifies a record that has no entry in the specified column.
b. There is no record that meets the Where condition.

The default value is checked against the comparison value.

**Where-condition**

The where condition is structured as follows:

> Selection of the table column that contains the name of the Customizing switch
> Comparison operator
> Criterion that is expected in the table column of the Customizing switch

Figure 316 shows an example of the query for determining whether the CHECK_S_USER_SAS Customizing switch fulfills the YES criterion in the PRGN_CUST table.

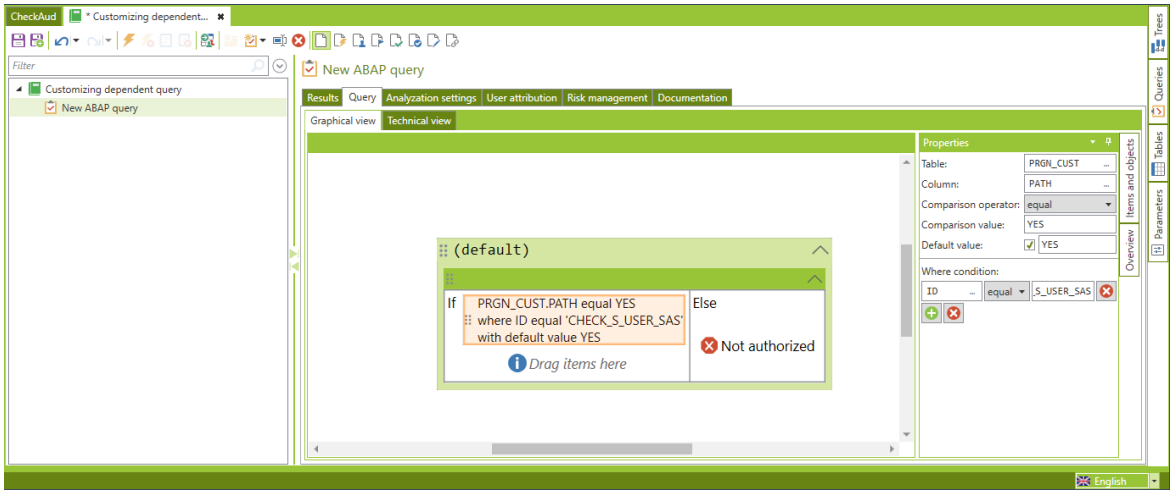



**Figure 316 - Customizing switch CHECK_S_USER_SAS**

### Structure of a Customizing-dependent - Technical view

The technical view represents component queries as follows:

```
{
 If
  <table> <table column> <relational operator> <comparison value>
  Where condition
  <table column><relational operator> <criterion>
  Optional
  <default value>
}
else
{
 …
}
```

**Example (Figure 316):** Query to determine whether the CHECK_S_USER_SAS Customizing switch fulfills the YES criterion (default value YES) in the PRGN_CUST table.

```
{
 if PRGN_CUST.PATH = 'YES' where ID = 'CHECK_S_USER_SAS' default 'YES'
 {
 }
}
```

### Examples of use

The following describes the example “The CHECK_S_USER_SAS Customizing switch” from the introduction using the CheckAud standard query “Assigning the SAP_ALL profile to users”.

First of all, check whether or not the S_USER_SAS authorization object is activated. Depending on the status of this authorization object, other authorization objects must then be checked. Please note that the S_USER_SAS authorization object is only activated by default for NetWeaver Release 7.31

or higher. A NetWeaver release check is therefore integrated into the IF operator (IF S_USER_SAS is active, else) in the first block (1 in figure 317)

The Customizing switch is checked similarly in both situations. The system searches for the comparison value YES in the PATH column of the PRGN_CUST table using the comparison operator “equal”. It does so under the condition that the CHECK_S_USER_SAS entry is available under the comparison operator “equal” in the ID column of the PRGN_CUST table.

The default value YES is applied in the following situations:

a. The Where condition identifies a record that has no entry.
b. There is no record that meets the Where condition.

The default value is checked against the comparison value.

Figure 317shows that an OR condition of the IF query is fulfilled. S_USER_SAS is therefore activated. This is indicated by the green checkmark (2 in figure 317). The section of the query that is not evaluated is grayed-out (see *Displaying with selected snapshot*).

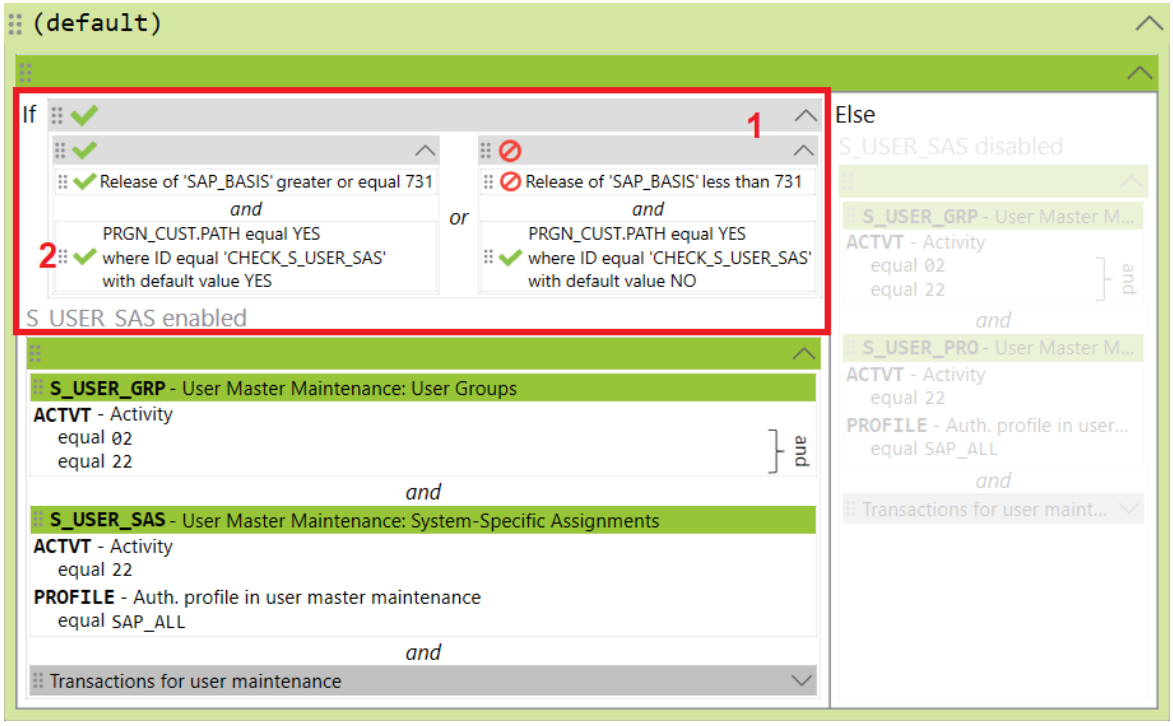



**Figure 317 - Table condition properties**

## V - 3.4.10 Dynamic field values in queries

### Introduction

Authorizations in an SAP system are usually adapted to the specific requirements of a company. As a result, there may be individual changes that may deviate from default values in the technical characteristics of authorizations. An example for this are the table authorization groups that are authorized using the S_TABU_DIS authorization object. The assignment of a table to a group can be changed for individual customers. Also, the group assignment may vary across different release versions.

The *Dynamic field values* function in queries can be used to dynamically identify and check field values for fields in authorization objects at runtime.

The *Dynamic field values* function in queries in the authorization object S_TABU_DIS is shown in (1) (Figure 318).

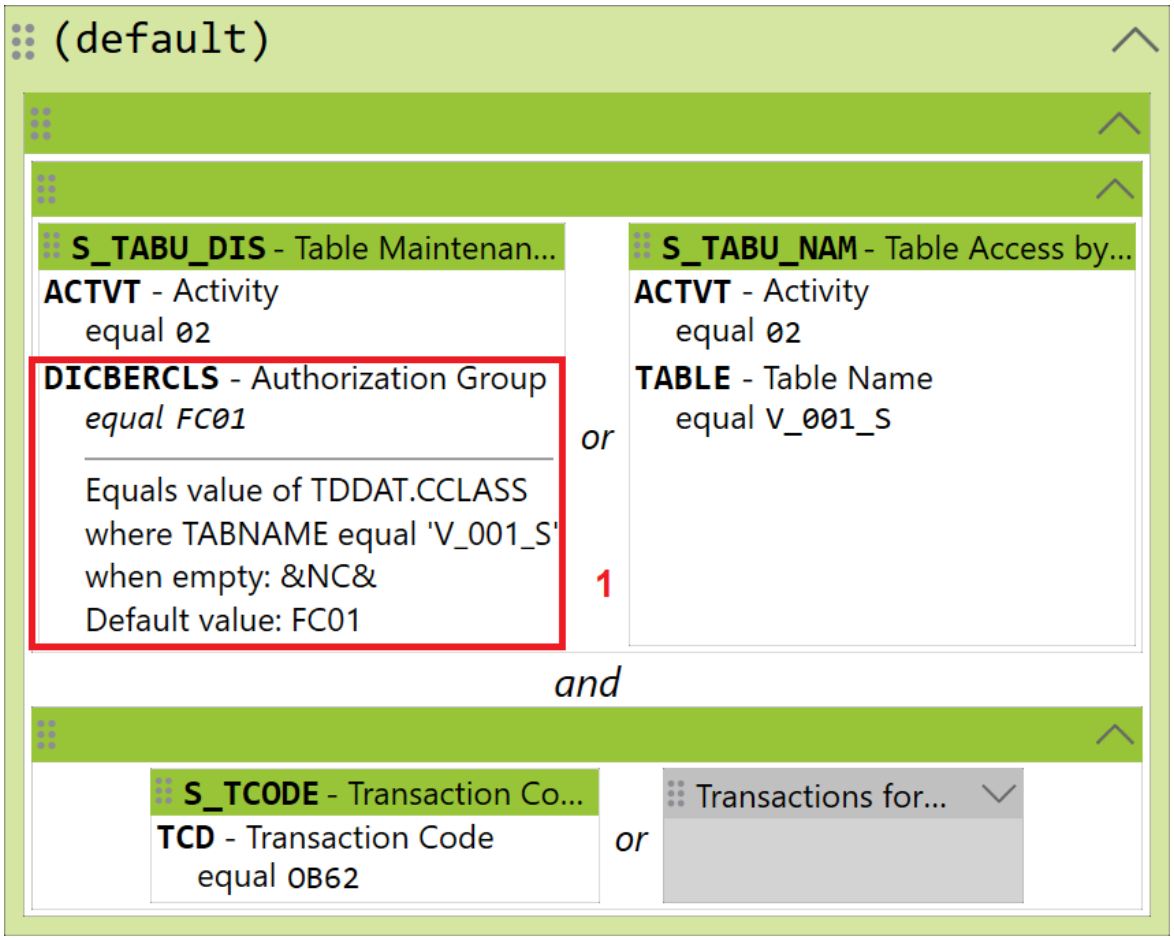



**Figure 318 - Dynamic field value in a query**

### Structure of a dynamic field value query - Graphical view

To create a dynamic field value query, drag an AND operator, for example, to the editing area in the design view of the authorization query (step 1 in figure 319). Then, drag an authorization object (here, S_TABU_DIS) to the *Drag elements here* area (step 2 in figure 319).


**Figure 319 - Inserting an AND operator in a query**

A field value is not automatically assigned to an authorization object by default. Click *No fields queried* to display the field values assigned to the authorization object (Figure 320)

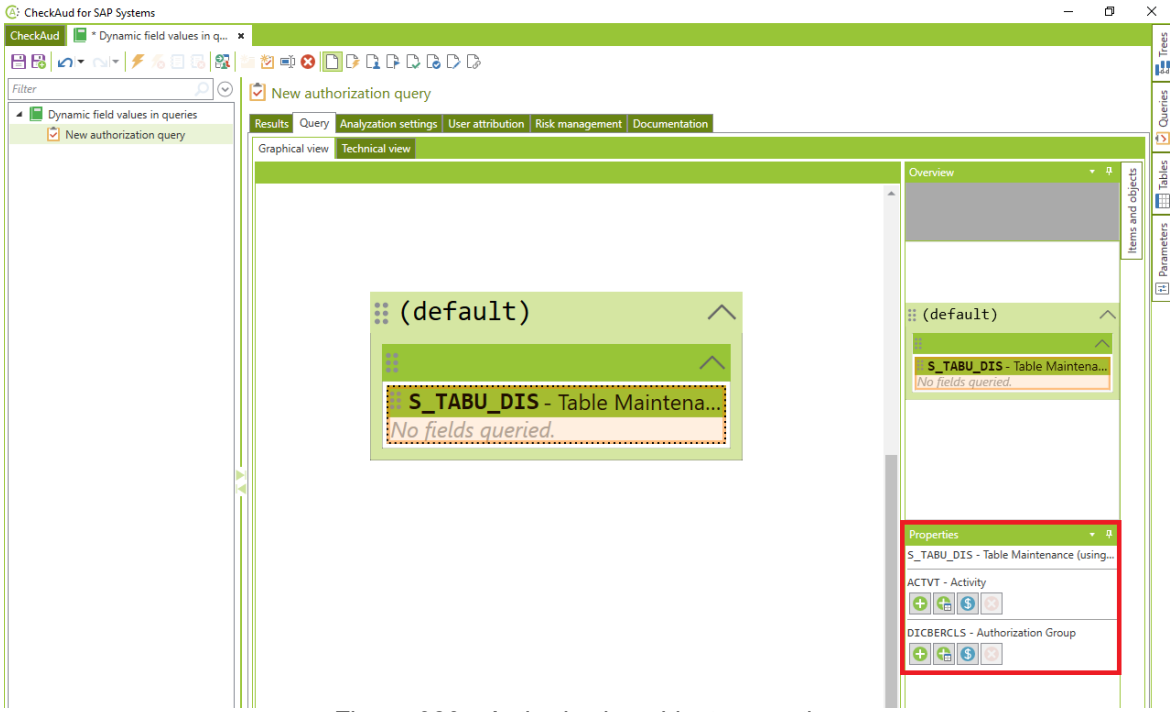



Figure 320 - Authorization object properties

A dynamic query value can be added using the icon. You can now configure the properties of dynamic field values (Figure 321).

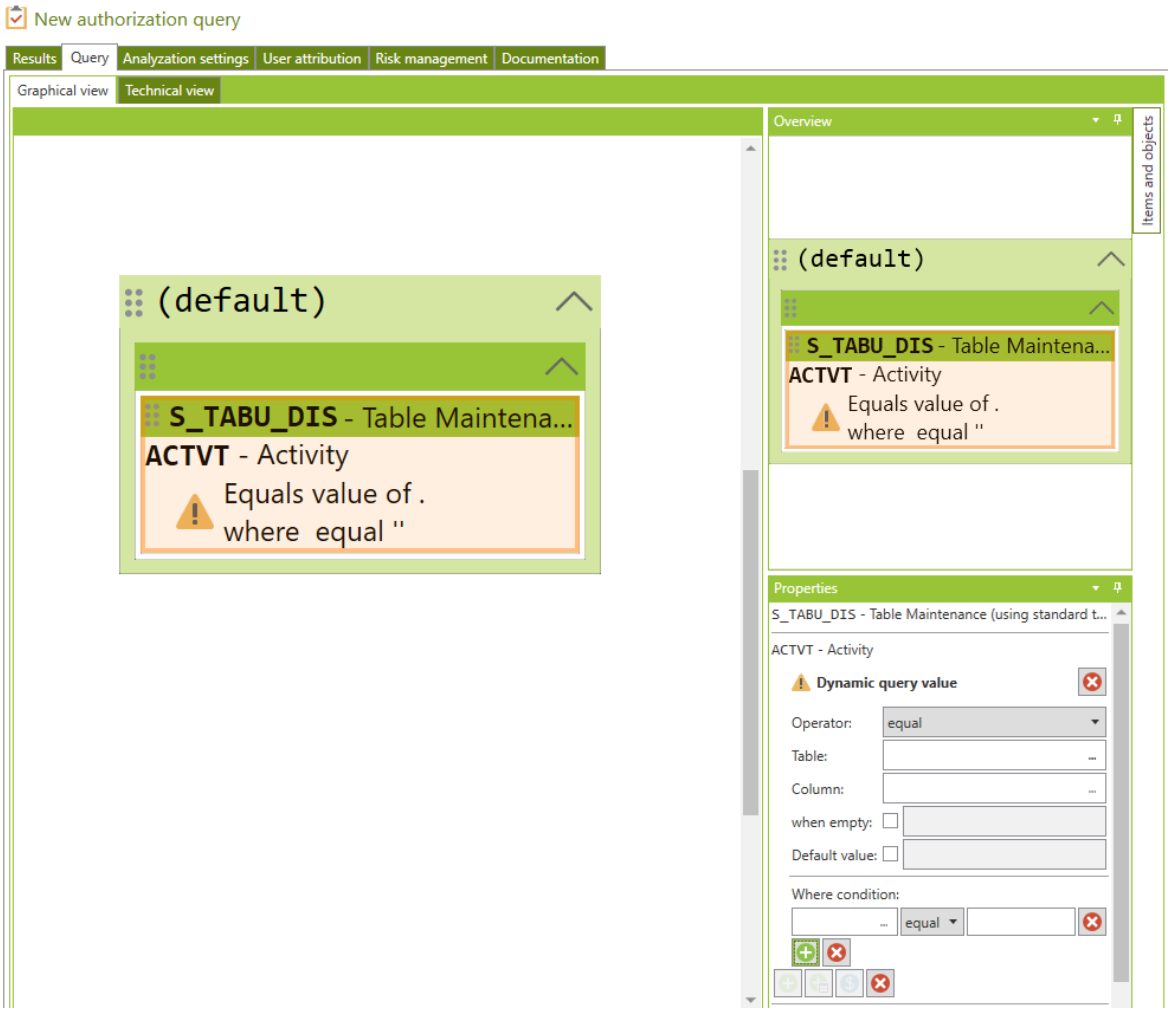



**Figure 321 - Creating a dynamic field value**

### Operator

Select one of the following options:

equal
any
all

### Table

Select the table that contains the value for the authorization object to be checked. To display suitable suggestions, you must first select a snapshot. All the tables included in the snapshot are then displayed.

### Column

The columns contained in the table selected in the previous step are displayed here. You can now select the column that contains the dynamic value for when a Where condition is successful. The value corresponds to the same row as the successful Where condition.

**When empty:**

The columns contained in the table selected in the previous step are displayed here. You can now select the column that contains the dynamic value for when a Where condition is successful. The value corresponds to the same row as the successful Where condition.

a. The Where condition identifies a record that has no entry in the specified column.
b. There is no record that meets the Where condition.

**Default value**

Select this checkbox to apply a specified default value. This default value is applied in the following situations:

a. The Where condition identifies a record that has no entry in the specified column.
b. There is no record that meets the Where condition.
c. The specified table or column is missing from the snapshot.

Note that the priority of “when empty” is higher than the default value.

**Where-condition**

The where condition is structured as follows:

> Selection of the table column that contains the name of the desired dynamic query
> Comparison operator
> Criterion that is expected in the table column

**Note:**

If multiple data records contain the criterion from the Where condition, the following rules apply:

a. When the operator is “equal,” the query cannot be evaluated.
b. When the operator is “any,” all the values are checked individually and then linked with “or” at authorization object level (example: found values 1;2 > 1 or 2).
c. When the operator is “all,” all the values are checked individually and then linked with “and” at authorization object level (example: found values 1;2 > 1 and 2).

Figure 322 shows an example of the dynamic search for the authorization group field value for the S_TABU_DIS authorization object.

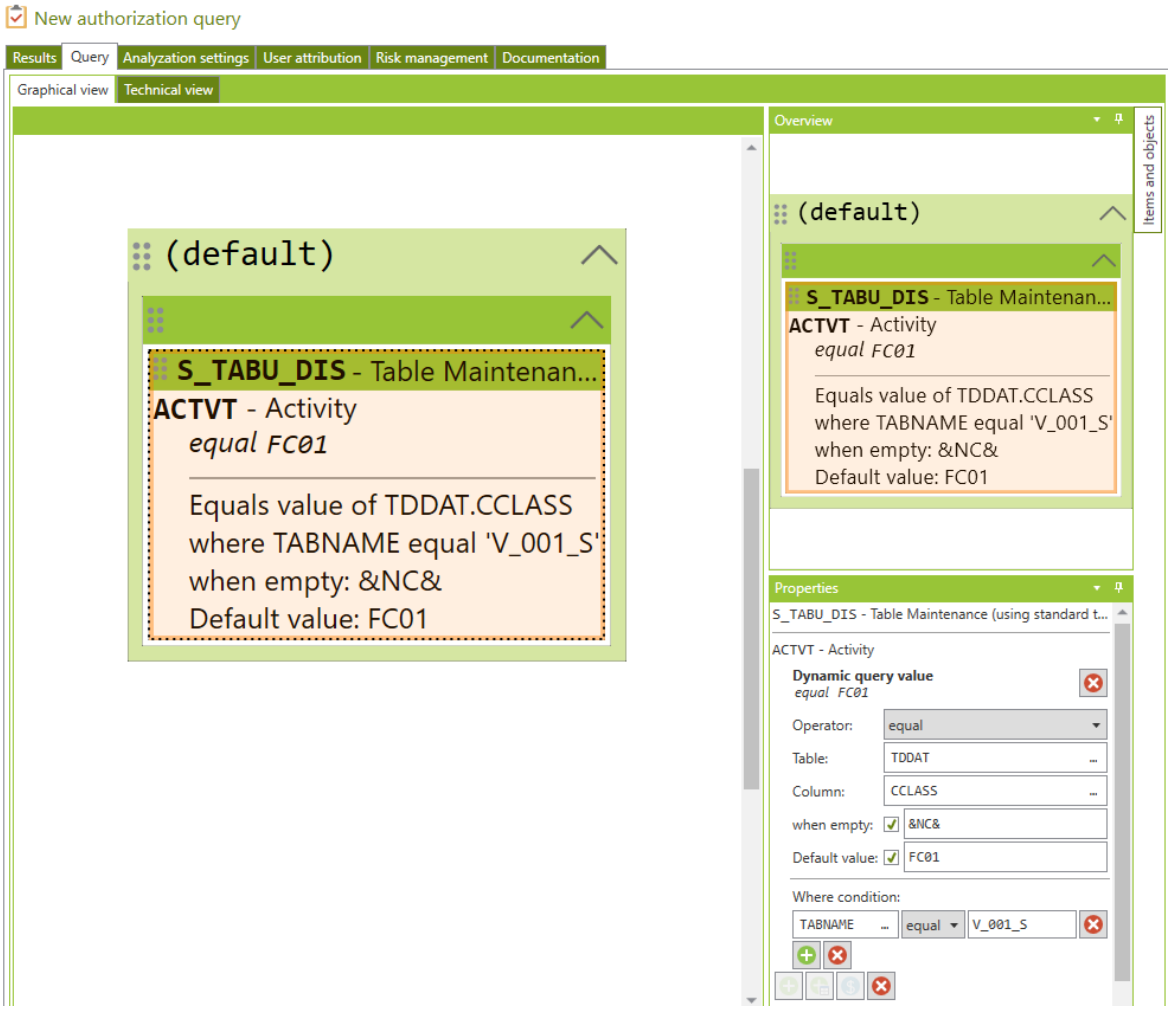



**Figure 322 - Properties of a dynamic field value query**

### Structure of a dynamic field value query - Technical view

The technical view represents component queries as follows:

```
{
<OPERATOR> <TABLE> <TABLE COLUMN>
WHERE CONDITION
<TABLE COLUMN><RELATIONAL OPERATOR> <CRITERION>
OPTIONAL
<WHEN EMPTY>
<DEFAULT VALUE>
}
```

### Example:

Which table authorization group is defined in the table TDDAT for the table V_001_S? With “when empty &NC&” & “default FC01”

```
{
 (
  S_TABU_DIS (ACTVT, DICBERCLS = select TDDAT.CCLASS where TABNAME = 'V_001_S' when empty '&NC&' defaul
 )
}
```

**Examples of use**

The subject of table authorization groups from the introduction will now be explained using the "Assign chart of accounts" query as an example. The S_TABU_DIS authorization object allows you to control access authorization for tables using the corresponding authorization group. You must therefore determine which table authorization group you want to check for the "Assign chart of accounts" query.

In the first block (1 in figure 323) the system checks whether the access authorization for tables is provided through the authorization objects S_TABU_DIS and/or S_TABU_NAM.

For the S_TABU_DIS authorization object, the check is carried out as follows:

In the TDDAT table, the system searches for all the data records that contain TABNAME='V_001_S' in the TABNAME column, with the operator "equal." If a data record is found, the value of the column CCLASS is extracted from this line as a dynamic query value (field value DICBERCLS (authorization group)).

The value for when empty (falls leer) is &NC&. It would be used in this example if:

a. The Where condition identifies a record that has no entry.
b. There is no record that meets the Where condition.

The default value is FC01. It would be used in this example if:

a. The specified table or column is missing from the snapshot.

After the query is executed with a specified snapshot, the result of the query appears under the field value (figure 323). ). In this example, the dynamic field value is FC01 and originates from the column CCLASS. The authorization object S_TABU_DIS in the Assign chart of accounts (Kontenplan zuordnen) query is therefore evaluated dynamically and the evaluation reflects the company's own assignments in its authorization system.

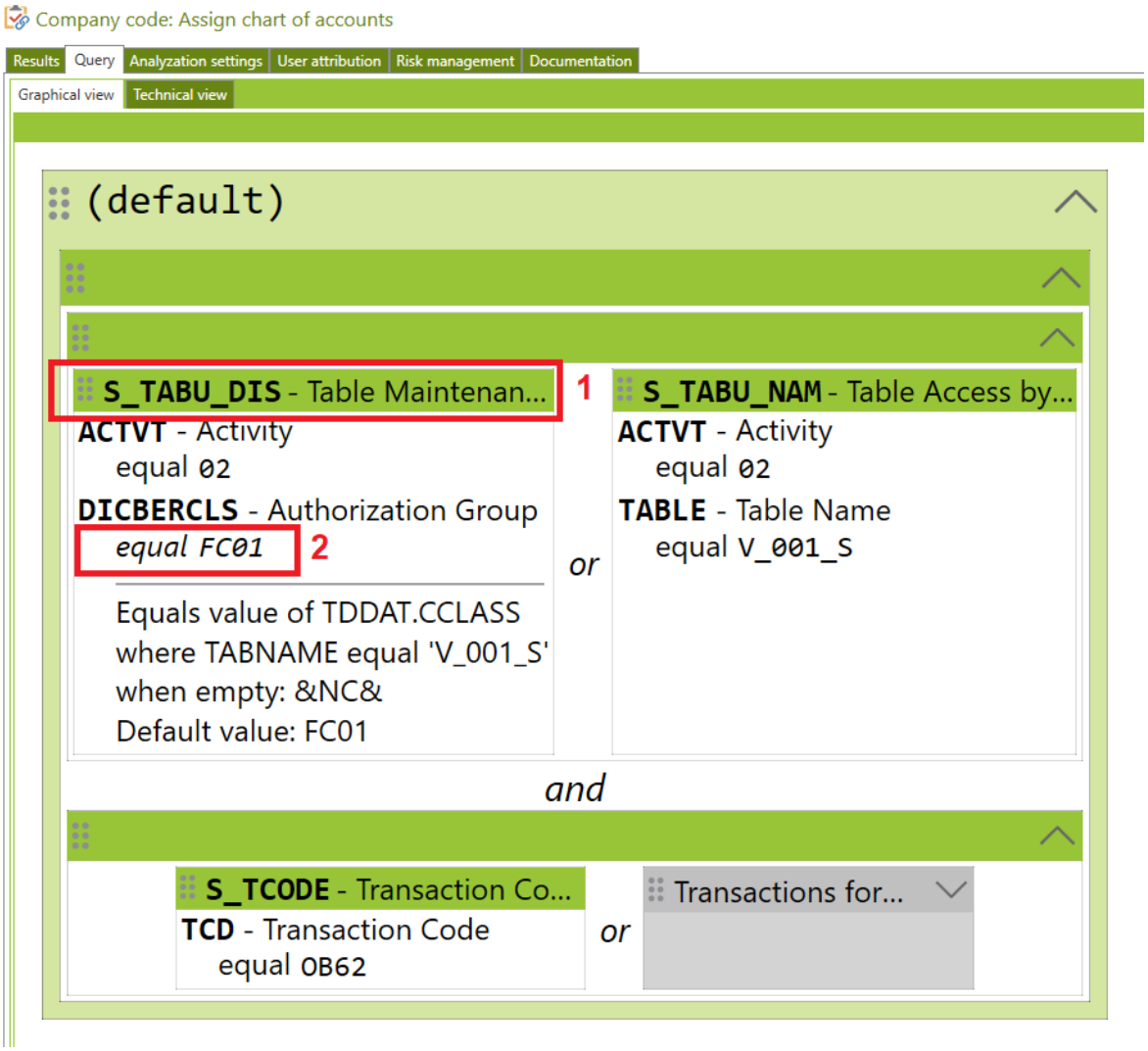



**Figure 323 - Properties of a dynamic field value query**

## V - 3.4.11 Adding app authorizations to the queries

### Introduction

The introduction of S/4HANA moves the use of apps in the SAP system to the foreground. Fiori and Legacy are probably the best known of these apps. The “role-based user experience” does not just involve changes for the user, but also some changes from an authorization perspective. While the classic authorization system primarily relied on transaction authorization, the focus is now on checking external services.

If, for example, a Fiori app is installed in the SAP system, a hash value is generated for this Fiori app and automatically added to the USOBHASH table. Contrary to transaction authorization, this hash value is then queried with the S_SERVICE authorization object.

The authorization queries in CheckAud are structured in such a way that the authorizations for installed apps can be checked with the S_SERVICE object.

The app query with the S_SERVICE authorization object is displayed in (1) (Figure 324).

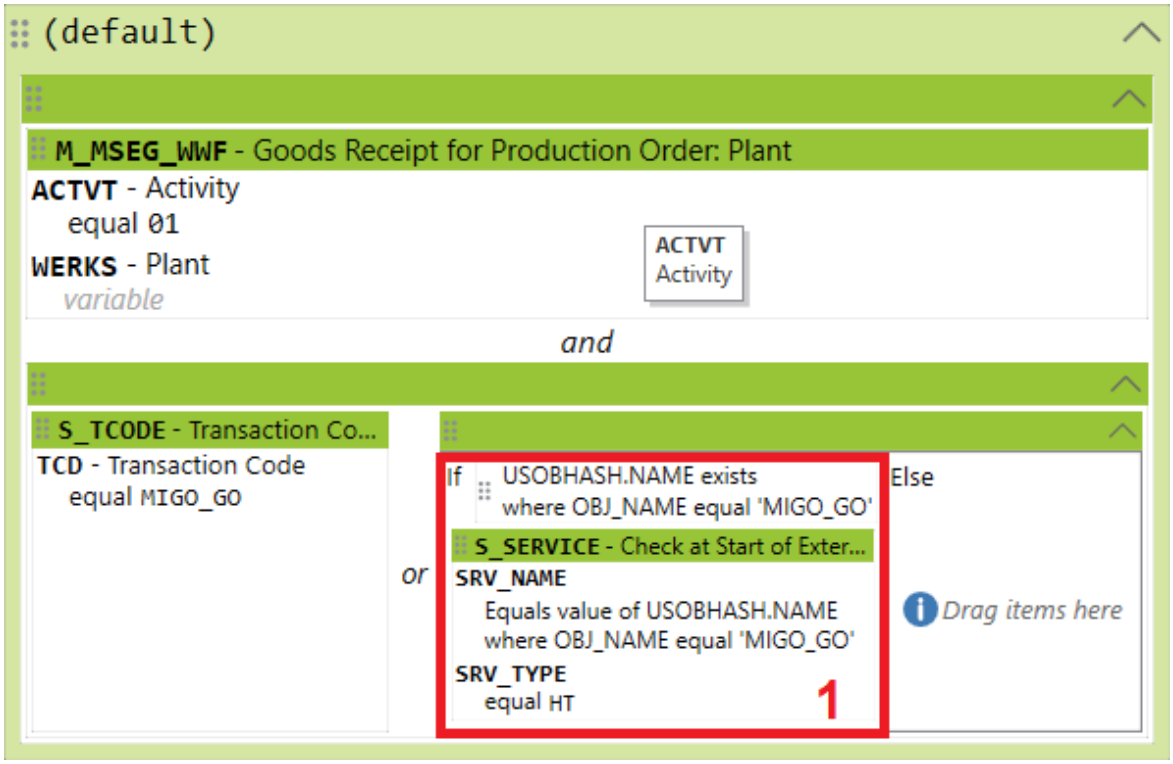



**Figure 325 - Authorization query for app authorization**

### App query structure using "Goods movement" as an example

Technically speaking, an app query is the combination of a Customizing-dependent query (see the chapter *Customizing-Dependent Queries*) with a dynamic query (see the chapter *Dynamic Field Values in Queries*).

After a hash value has been generated during the APP installation, the hash value is saved in the USOBHASH table. This hash value is then queried with the S_SERVICE authorization object. The process is as follows:

In the USOBHASH table, the Customizing-dependent query is used to determine whether the app is installed (1 in Figure 326). In this process, the system searches for the value MIGO_GO in the OBJ_NAME column of the USOBHASH table. If this value is found, the system checks whether a hash value exists in the NAME column of the USOBHASH table. If a hash value is available, the query check is deemed successful.

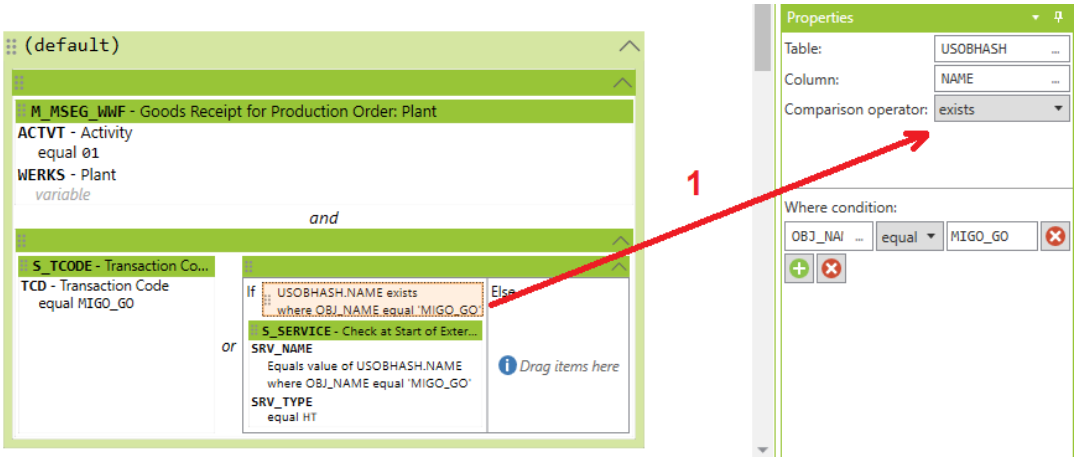



**Figure 326 - App query (Customizing-dependent query)**

If the app is installed, the dynamic query uses the USOBHASH table to determine the hash value that is assigned to the app. The value is then assigned to the S_SERVICE authorization object (2 in Figure 327). In this process, the system searches for the value MIGO_GO in the OBJ_NAME column of the USOBHASH table. If this value is found, the system determines the hash value in the NAME column of the USOBHASH table. The hash value is then applied to the SRV_NAME field value of the S_SERVICE authorization object. The TYPE of the check indicator must be HT; therefore, the operator for the SRV_TYPE field value is “equal”.

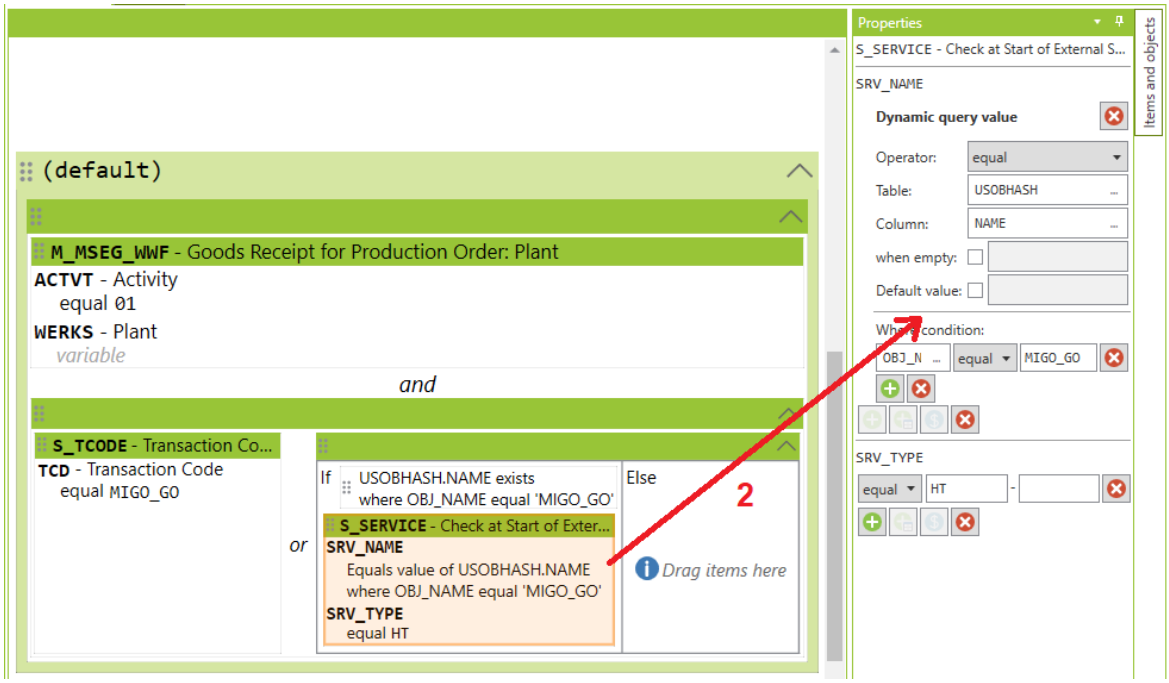



**Figure 327 - App query (dynamic query)**

The hash value determined for the S_SERVICE authorization object is used for the authorization check.

## V - 3.5 Authorization queries (HANA DB)

### V - 3.5.1 Create/Changing own queries - graphical view

Creating or changing HANA DB queries works the same way as described in chapter Create/Changing own queries - graphical view 212 for ABAP queries. Only type and scope of the available query elements will differ on HANA DB queries.

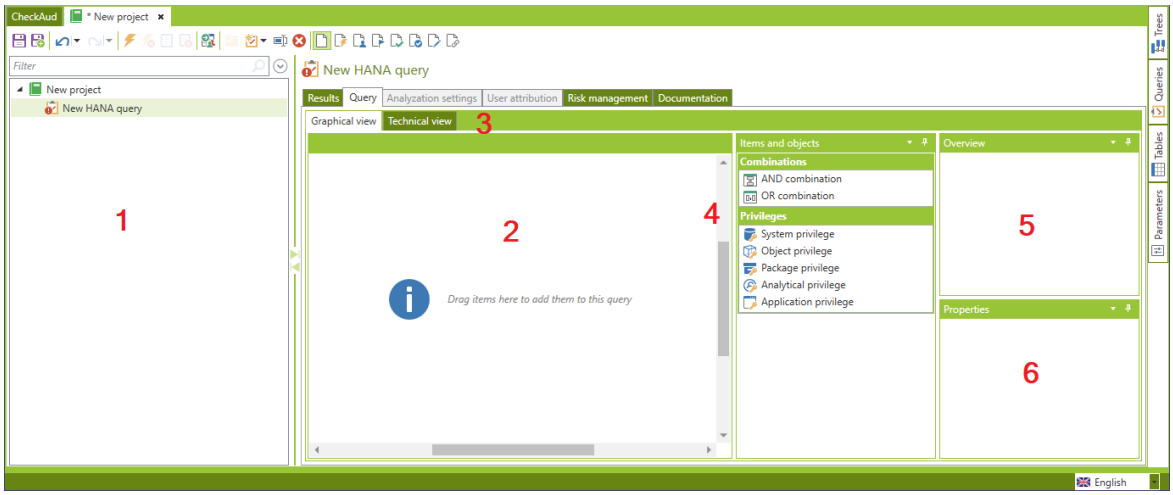
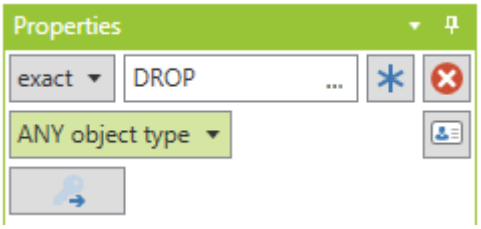
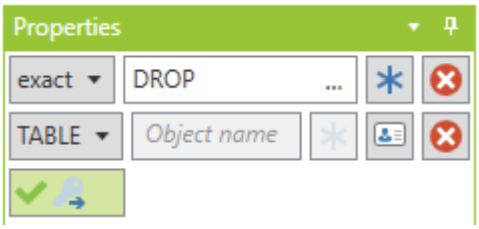


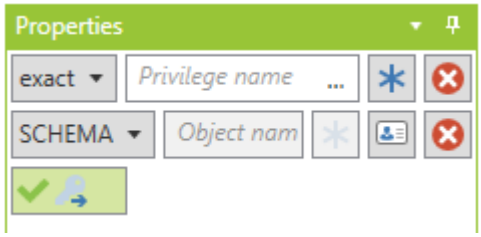

**Figure 328 - Editor for modifying authorization queries (HANA DB)**

1. New query in the analysis project
2. Editor area, graphical view of the composition of the authorization
3. Editor area, text view of the composition of the authorization
4. Toolbox for selecting logical connectives and privileges
5. Overview of the graphical view of authorization compositions
6. Editing box for editing the field values/properties of the authorization object selected in the editor area

With the specification "EXCLUDE USER SCHEMAS" all permissions on schemas whose name is identical to the authorized user (= "user schema") can be excluded from the analysis. This option can be used exclusively when either checking for "ANY object type" or when checking for a schema or a schema-bound object using the ANY operator (i.e. not checking for a concrete name).



### V - 3.5.2 Create/Changing own queries - technical view

Auch bei HANA DB Abfragen kann alternativ kann für die Erstellung von Berechtigungsabfragen der Texteditor genutzt werden. Hierfür muss von der Grafischen Ansicht in die Technische Ansicht gewechselt werden.

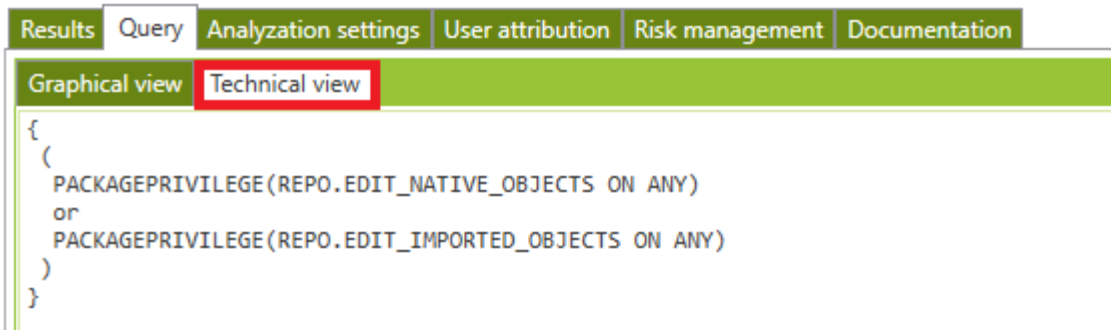



**Figure 329 - technical editor for modifying authorization queries (HANA DB)**

### V - 3.5.3 Logical connectives for queries

For HANA DB queries, the same connectives ar available as described in chapter Logical connectives for queries 225. Only the *EXCEPT* connective is not available for HANA DB queries.

### V - 3.5.4 Authorization types

With the toolbox *Privileges* the different types of HANA DB authorizations can be used in the graphical editor via Drag & Drop on the logical container.

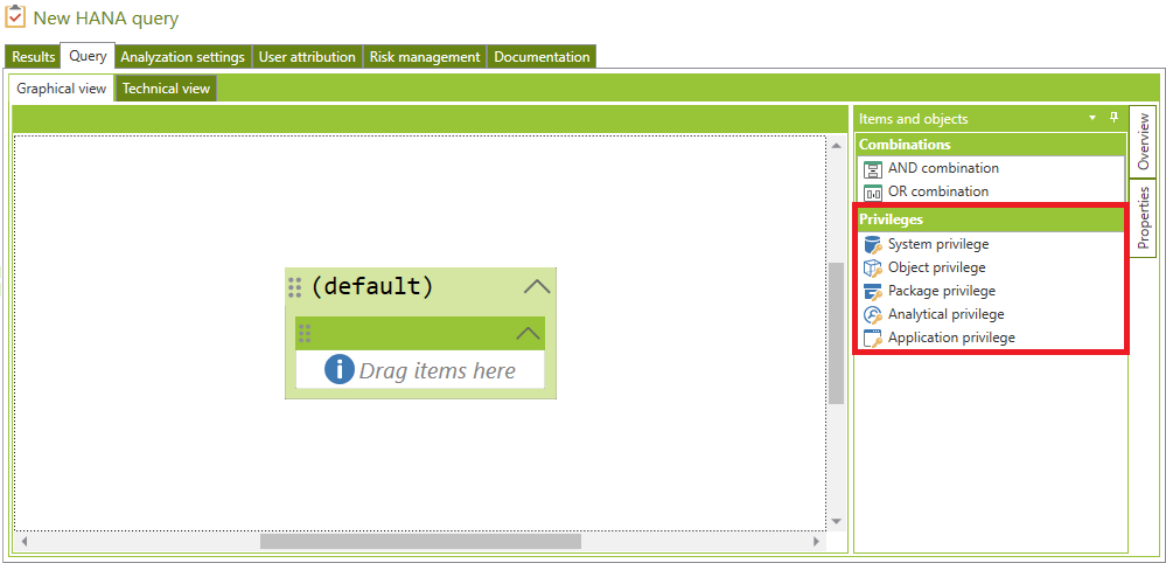



**Figure 330 - HANA DB authorization types**

**System privilege:**
With system privileges the access for database maintenance will be given (e. g. administration of schema, users, catalog roles, backup activities). The typical user group for system privileges are the database administrators. The HANA standard users SYSTEM and _SYS_REPO already have all system privileges by standard.

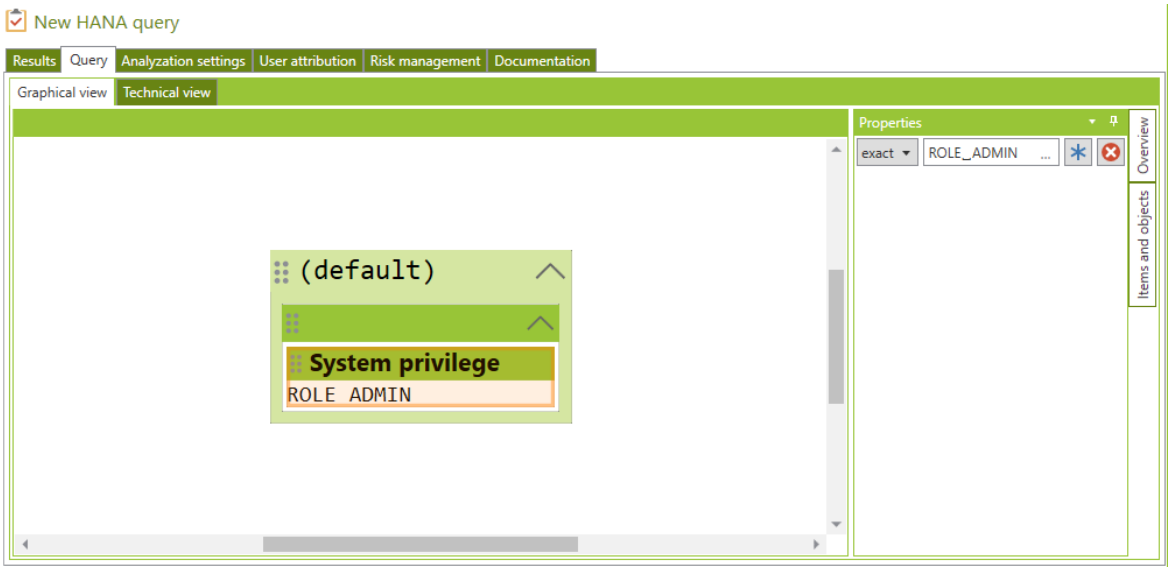



**Figure 331 - HANA DB query for system privileges**

### Object privilege:

With object privileges the access for database objects will be given (e. g. schema, tables, views and procedures). For every SQL command (e. g. SELECT, UPDATE, EXECUTE) there exists an own object privilege. A user, who wants access to tables, needs an object privilege for this particular table or the superior schema. Object privileges can be granted for catalog objects or repository objects.

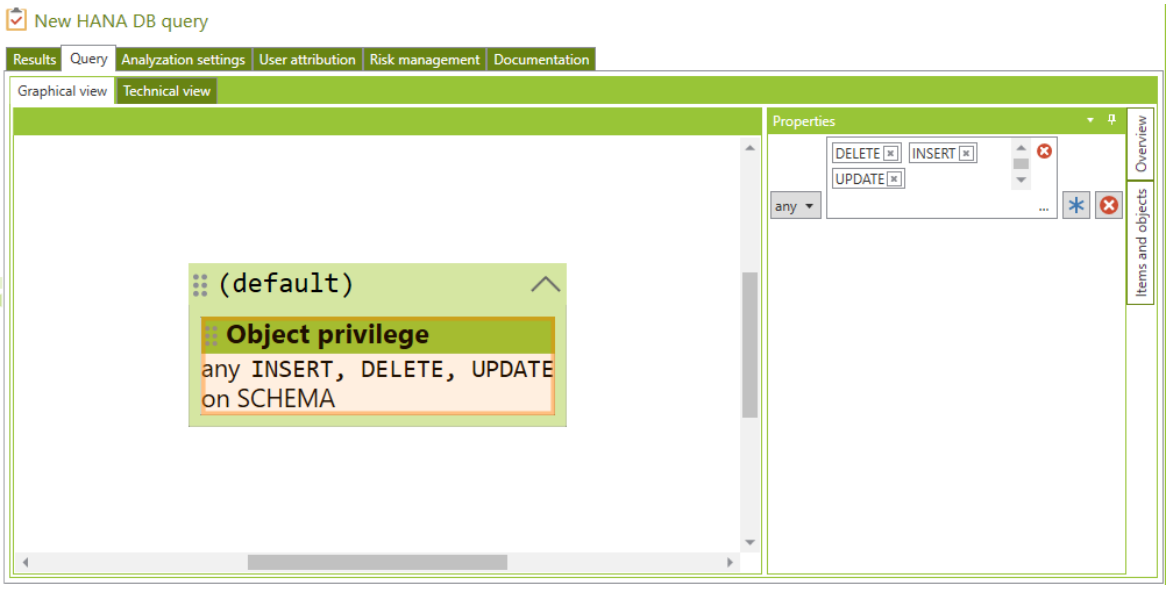



**Figure 332 - HANA DB query for object privileges**

### Package privilege:

With package privileges the access for development environment will be given. The development environment is devided into logical associated objects, which are called packages. A user with with a package privileg for a repository package is automatically authorized for all containing objects and sub-packages.

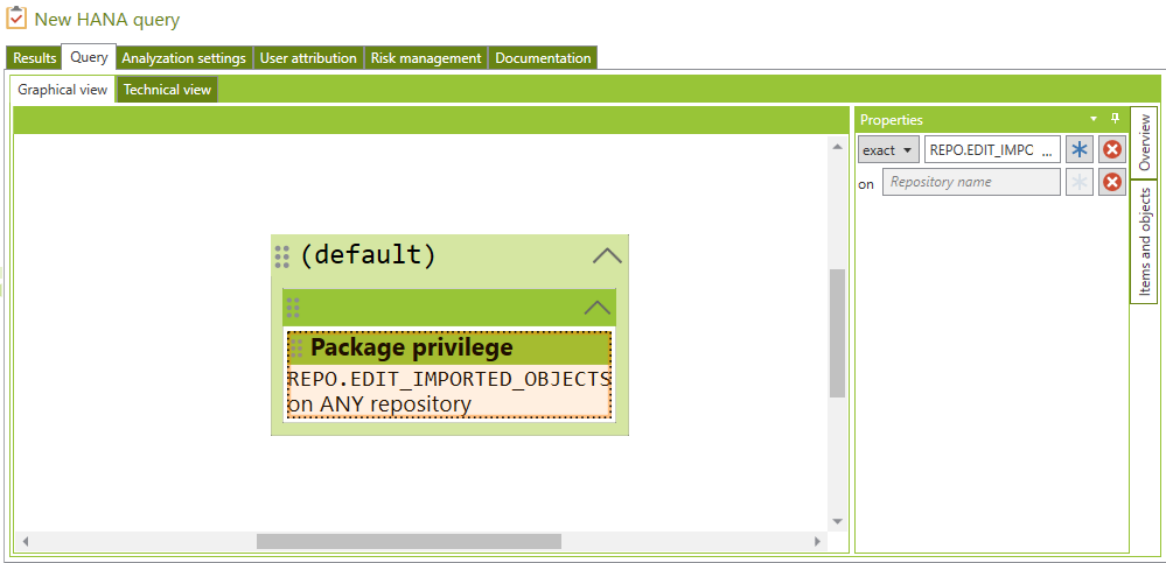



**Figure 333 - HANA DB query for package privileges**

### Analytical privilege:

With analytical privileges access for application data will be given (e. g. analytical views, attribute views, calculation views). This regulates the access of users to the application data. The access will be granted with a rowbased authorization. Therefore a organizational seperation ist possible. Also a period of validity can be defined with analytical privileges.

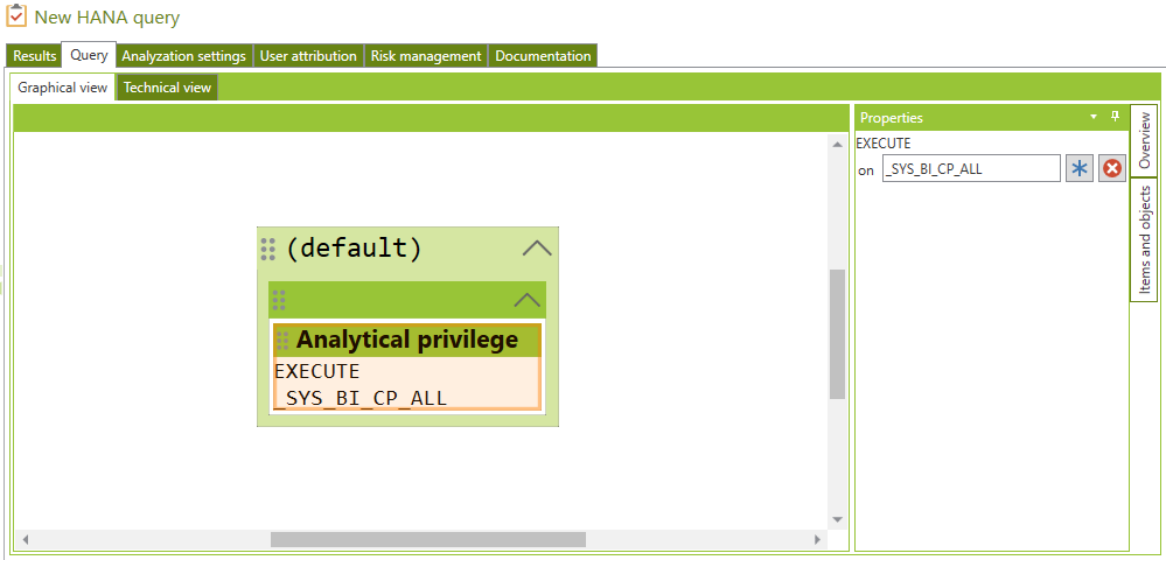



**Figure 334 - HANA DB query for analytical privileges**

### Application privileges:

With application privileges the access of SAP HANA XS applications (Extended Services) will be given. The authorizations will be defined in the package, in which the application is located. Application privileges have user defined names which are stored in a file with a defined name *.xsprivileges*.

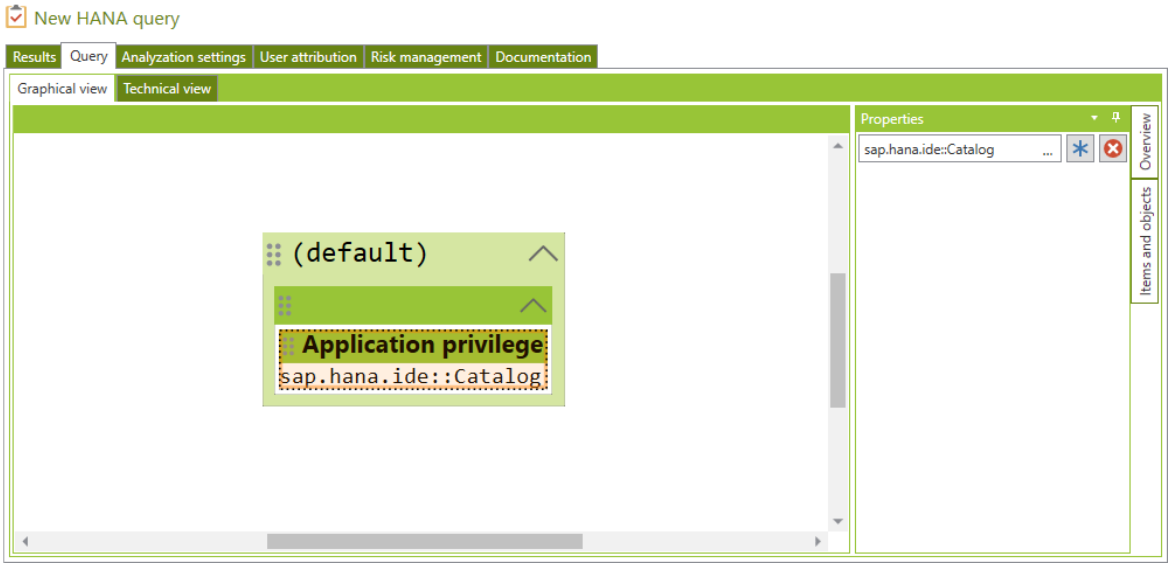
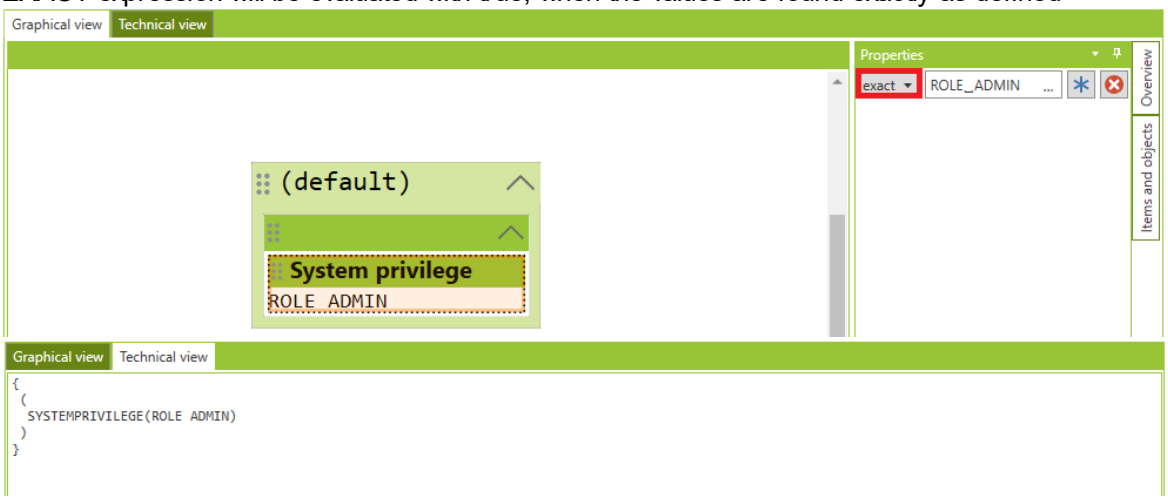



**Figure 335 - HANA DB query for application privileges**

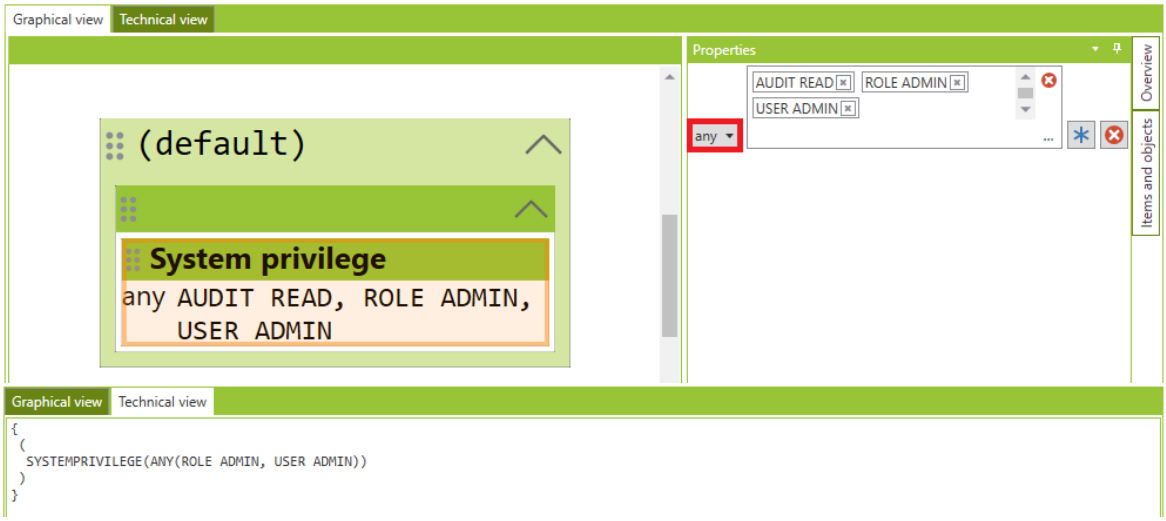
### V - 3.5.5 Relational operators for authorization types

Depending from the authorization type, there are differnt relational operators, which can be used:

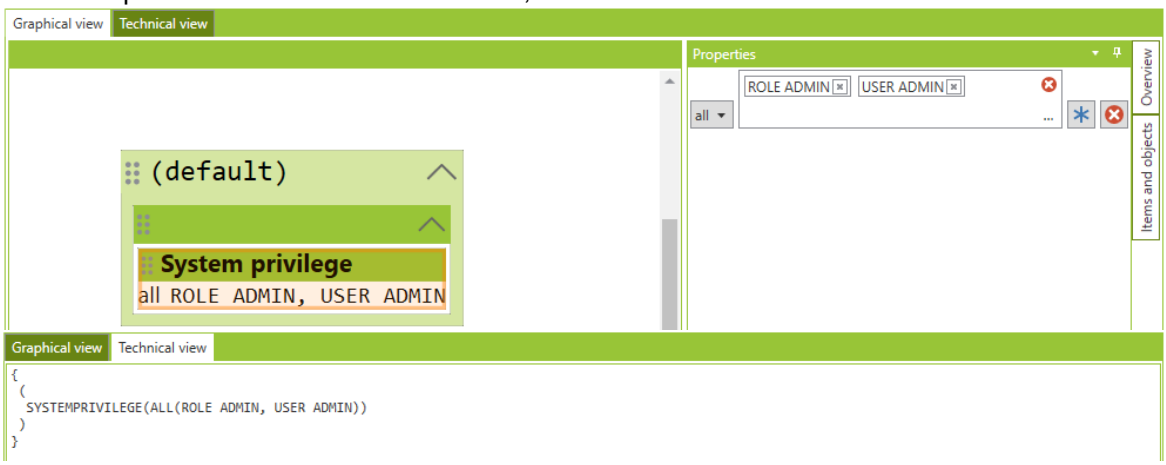
EXACT expression will be evaluated with true, when the values are found exactly as defined



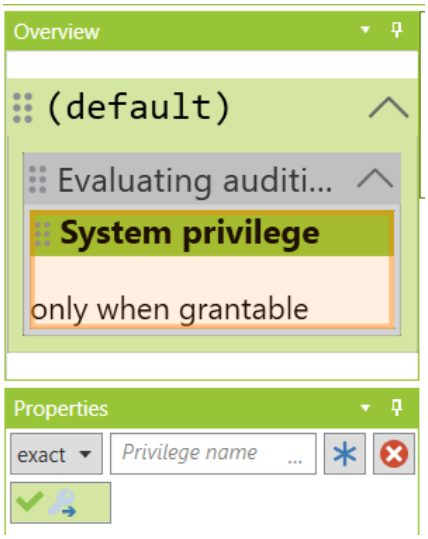

ANY expression will be evaluated with true, when parts of the values are found




ALL expression will be evaluated with true, when all of the values are found




In the properties windows of system, object and package permissions "only grantable permissions" are included as a criterion.




## V - 4 Working with tables and table queries

By using table sets, you can read out any SAP tables or HANA database tables. The read-out tables can be accessed using the toolbox *Tables*. In this toolbox, the tables are displayed separated in systems and table sets.

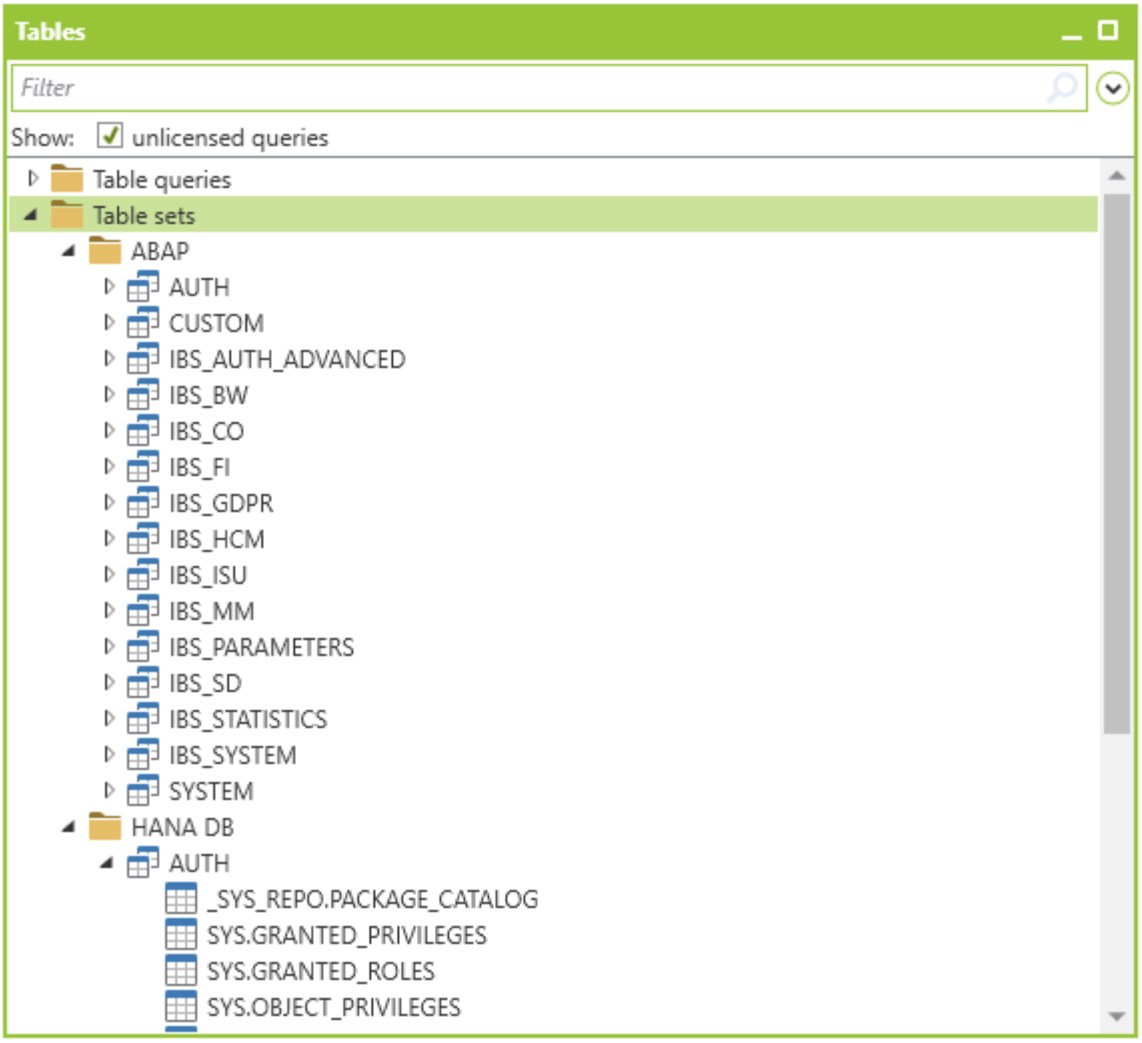



**Figure 336 - Selecting the available ABAP or HANA DB tables based on table sets**

You can select the individual tables and drag and drop them into the analysis project.

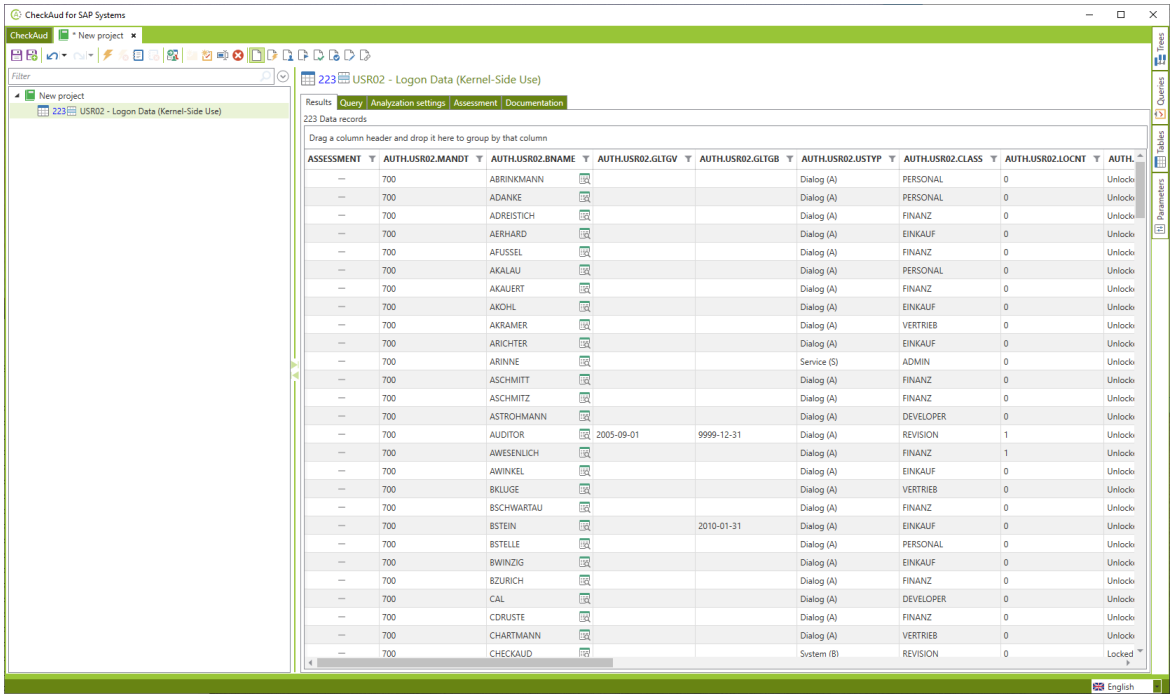



**Figure 337 - Evaluating the selected table**

After CheckAud has completed the analysis, the contents of the selected table are listed.

## V - 4.1 Predefined table queries

The predefined table queries are an extension of the table display. By linking several tables and using table joins and filter selections, you can create specific queries for the tables.

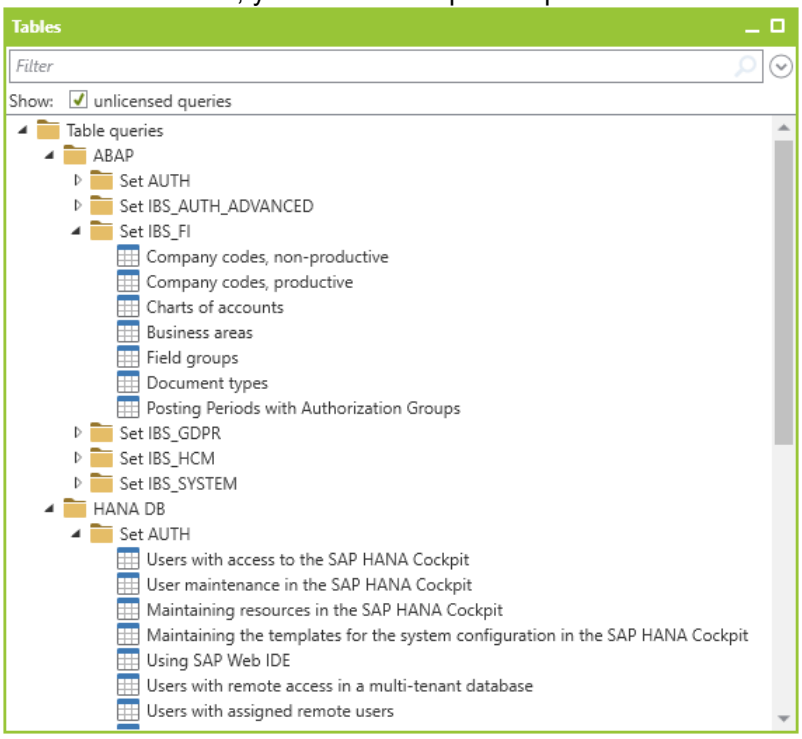



**Figure 338 - Predefined table queries**

You can drag and drop predefined table queries into your project.

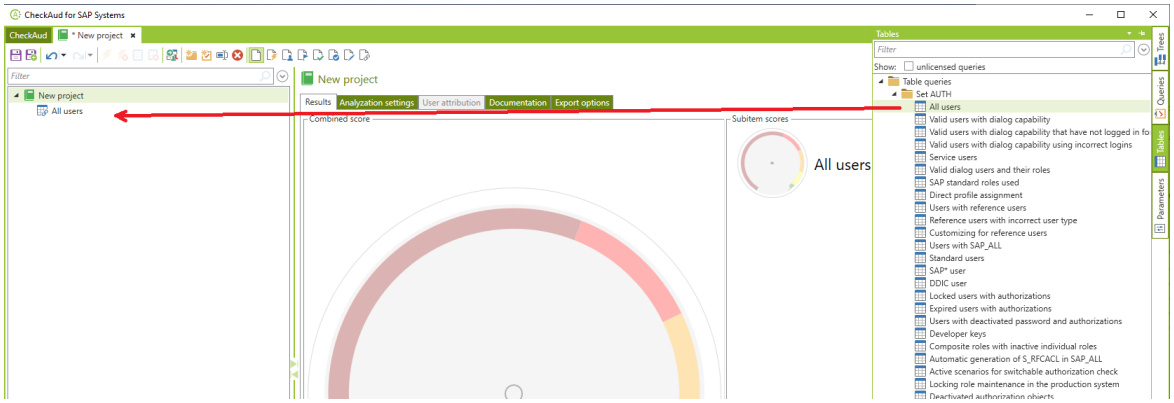



**Figure 339 - Inserting a predefined table query**

## V - 4.2 Creating own table queries

The tables stored in the snapshot from the SAP system or HANA database cannot only be analyzed using CheckAud and the stored queries; it is also possible to link tables together to provide information from multiple tables aggregated into one view. To link tables together, a table must be included in the analysis project first. Following examples are showing the procedure for creating SAP (ABAP) table queries. It can also be used for creating similar queries for HANA database tables.

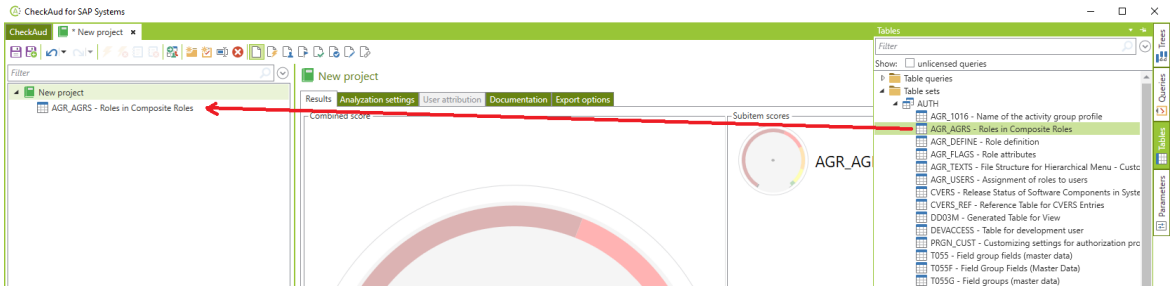


**Figure 340 - Adding a table**

After adding the desired table, select it. You can then add another table to the existing one on the *Query* tab. Here, the second table is selected from the table sets and inserted next to the existing table. Combining two tables is done via the drag and drop function. The  button indicates that the table can be inserted.

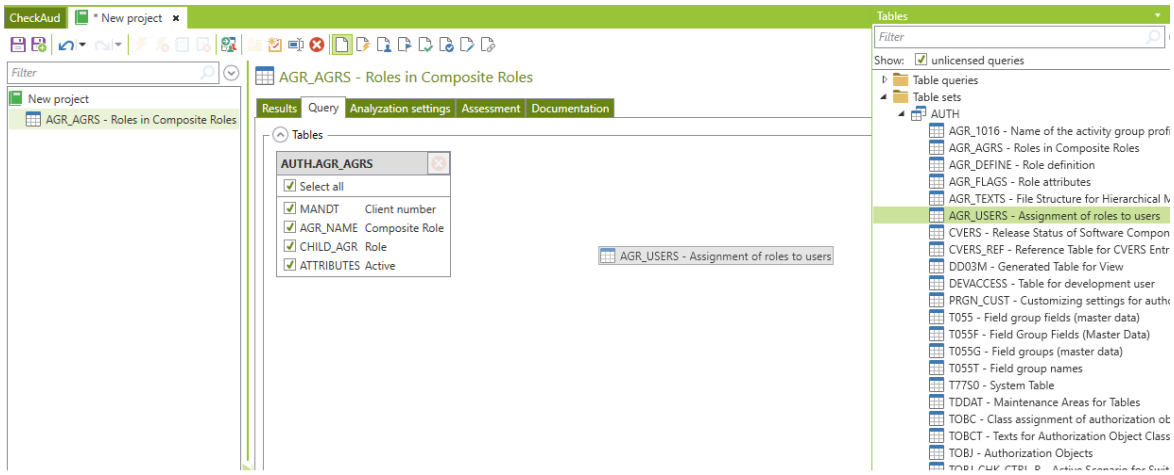


**Figure 341 - Linking two tables**

Once the desired tables are combined, the contents of the result display can be defined. This is done by selecting the fields of the respective tables.

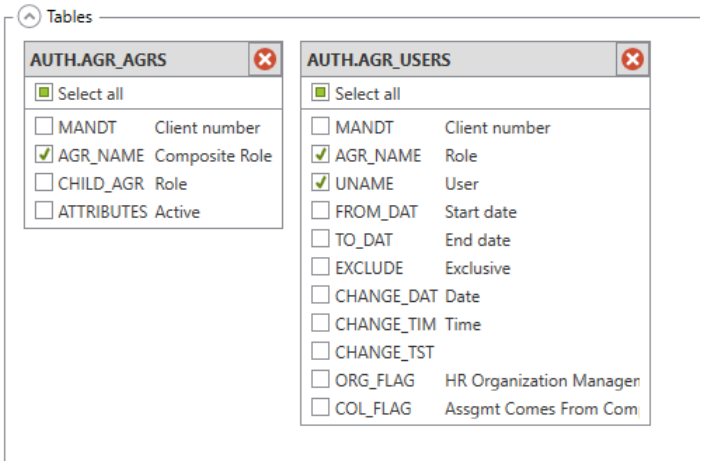



**Figure 342 - Field selection for the linked tables**

The next step is linking the tables using table joins. The four ways to link tables are described below with reference examples.


**Figure 343 - Defining JOINS**

Using the selection feature, the contents of the result can be restricted.

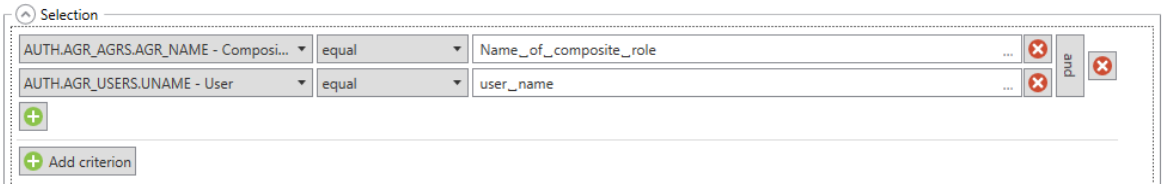



**Figure 344 - Selecting the contents of a JOIN**

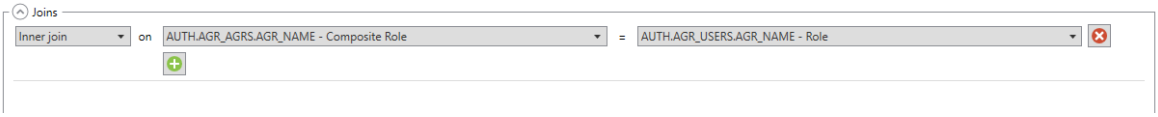
**Setting up an INNER JOIN:**

Explanation: The INNER JOIN joins records from the left and right tables precisely when the criteria specified under JOIN are all met. If one or more of the criteria are not met, no record is created in the result set.

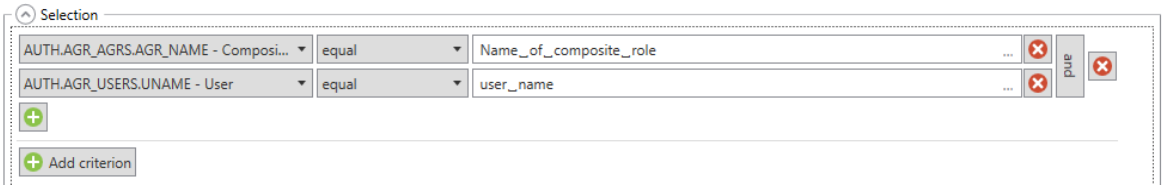
Example: Displaying assignment via user composite roles

Procedure: Insert the AGR_AGRS table in the project. Then select the AGR_AGRS table in the project and return to the *Query* tab. In the next step, the AGR_USERS table is combined with the existing table. Next, the join is set up.

JOIN:



Filter results:




Using the selection feature, the content of the result can be restricted. In the example, the result is limited to a composite role and a user name.

Result: The system displays all the composite roles that are assigned to a certain user.

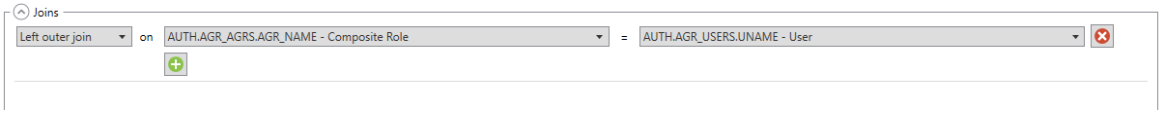
**Setting up a LEFT OUTER JOIN:**

Explanation: A record from the left table is always included in the result; therefore, the resulting table has as many records as the left table. If a record from the right table corresponds to the join criteria, it is registered accordingly in the column; otherwise the columns remain empty.

Example: Display of users to whom no role has been assigned.

Procedure: Insert the USER_ADDRS table in the project. Then select the USER_ADDRS table in the project and return to the *Query* tab. In the next step, the AGR_USERS table is combined with the existing table. Next, the join is set up.

JOIN:




Filter results:


The selection filter must be AGR_NAME = “empty,” so that all users without a role assignment are displayed.

Result: All users without a role assignment are displayed.

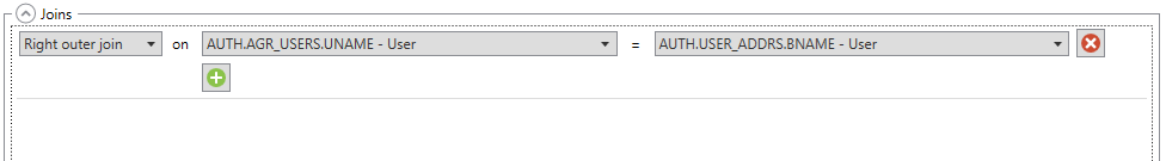
**Setting up a RIGHT OUTER JOIN:**

Explanation: The RIGHT OUTER JOIN is the reverse of the LEFT OUTER JOIN. A record from the right table is always included in the result; therefore, the resulting table has as many records as the right table. If a record from the link table corresponds to the join criteria, it is registered accordingly in the column; otherwise the columns remain empty.

Example: Display of users to whom no role has been assigned.

Procedure: Insert the AGR_USERS table in the project. Then select the AGR_USERS table in the project and return to the *Query* tab. In the next step, combine the USER_ADDRS table with the existing table. Next, the join is set up.

JOIN:




Filter results:


The selection filter must be AGR_NAME = “empty” so that all users without a role assignment are displayed.

Result: All users without a role assignment are displayed.

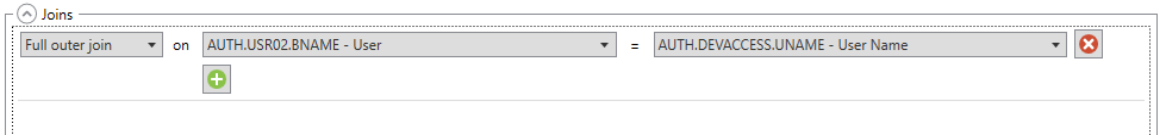
**Setting up a FULL OUTER JOIN:**

Explanation: This join is a combination of the LEFT and RIGHT OUTER JOIN. Each record from the right and left table is included in the result set. If the JOIN criterion finds a suitable partner, they are linked; otherwise, each missing page is left blank.

Example: Displaying all user names with master records and/or developer keys

Procedure: Insert the USR02 table in the project. Then select the USR02 table in the project and return to the *Query* tab. In the next step, combine the DEVACCESS table with the existing table. Next, the join is set up.

JOIN:




Filter results:


The selection filter must be “DEVACCESS ≠ “empty” so that all users with developer keys are displayed.

Result: All users with developer keys are displayed.

## V - 4.3 Table queries for tables that are not fully read out

If table queries that you created yourself access tables that may not have been fully read out (due to filters in the table set or activated anonymization/pseudonymization), this is indicated by a message in the displayed results.

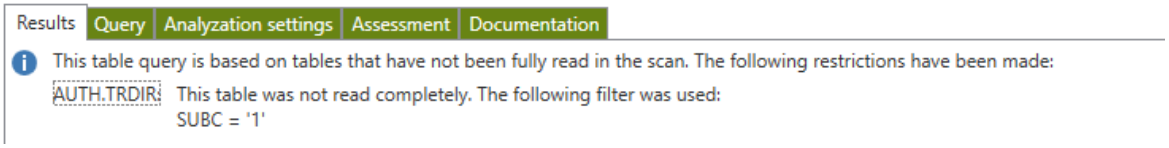



**Figure 345 - Message when a table was not fully read out due to an active filter in the scan table set**

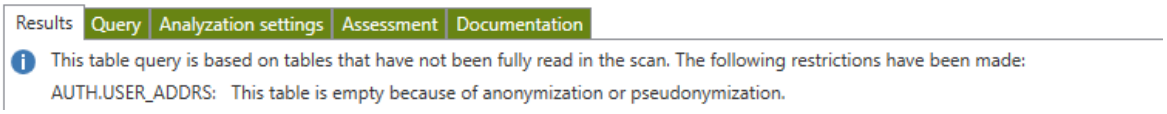



**Figure 346 -Message when a table was not fully read out due to active anonymization/pseudonymization in the scan table set**

## V - 4.4 Creating aassessment criteria for tables/table queries

In addition to simply displaying the results, you can also define an assessment. You do so on the *Assessment* tab page

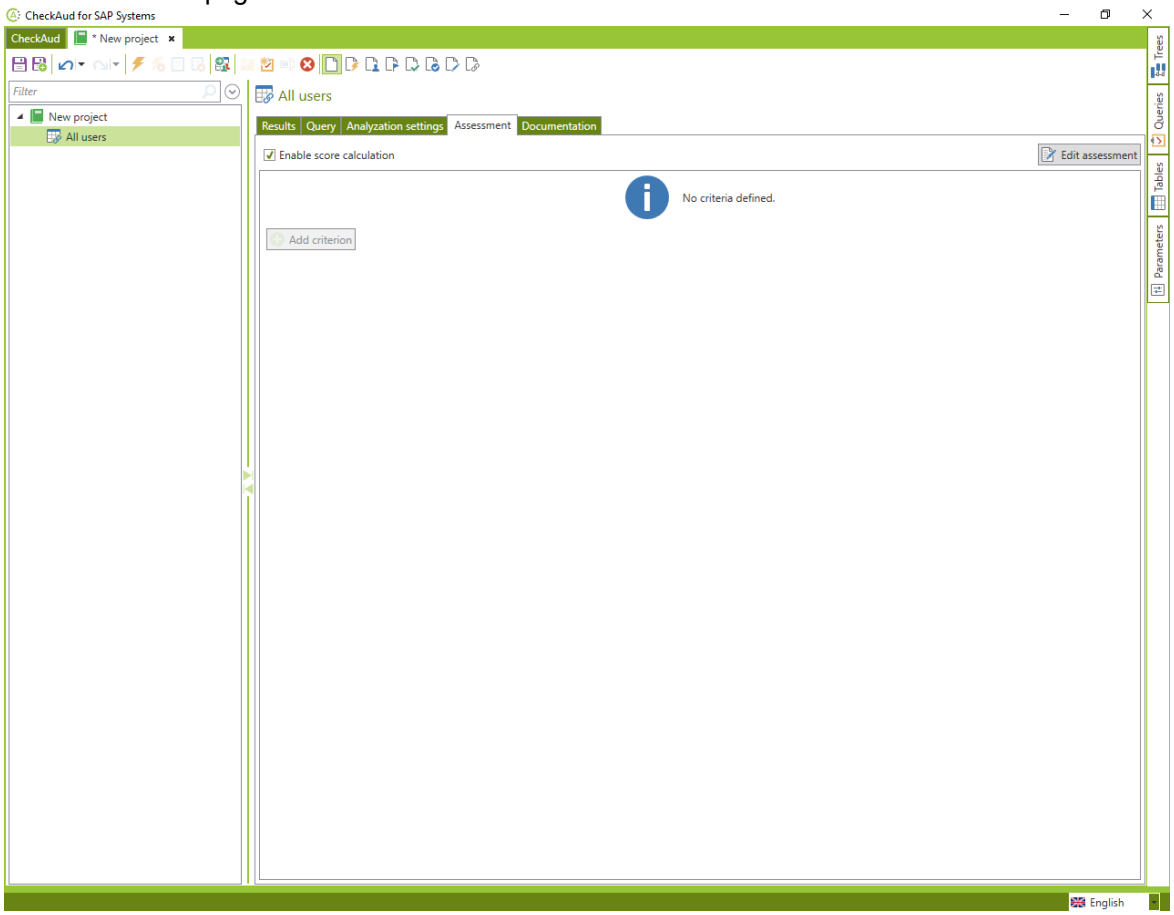



**Figure 347 - Assessing the table query**

The assessment comprises individual filter criteria that are linked using AND or OR operators in the same way as the selection criteria on the *Query* tab page. If the assessment criteria for a record are fulfilled, it is highlighted in the results list accordingly. If you have not defined any criteria, a - is displayed for all the records in the assessment column.

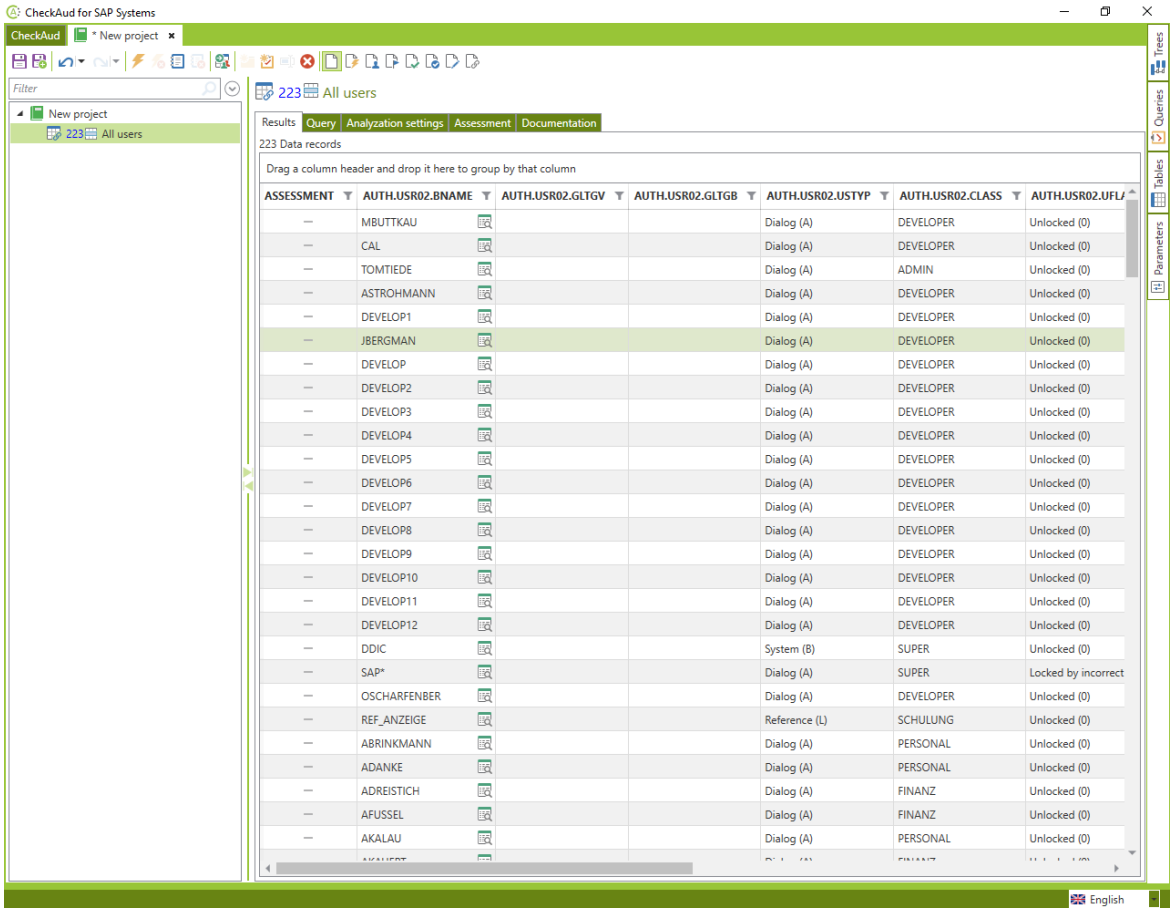



**Figure 348 - An assessed table query**

The system can assess all columns that form part of the result set. It is also possible to assess the number of records present in the result set. For example, it is conceivable that a table query may not contain any results. In this case, you can simply set the assessment criterion for COUNT to the value 0 (with the operator “equal”).

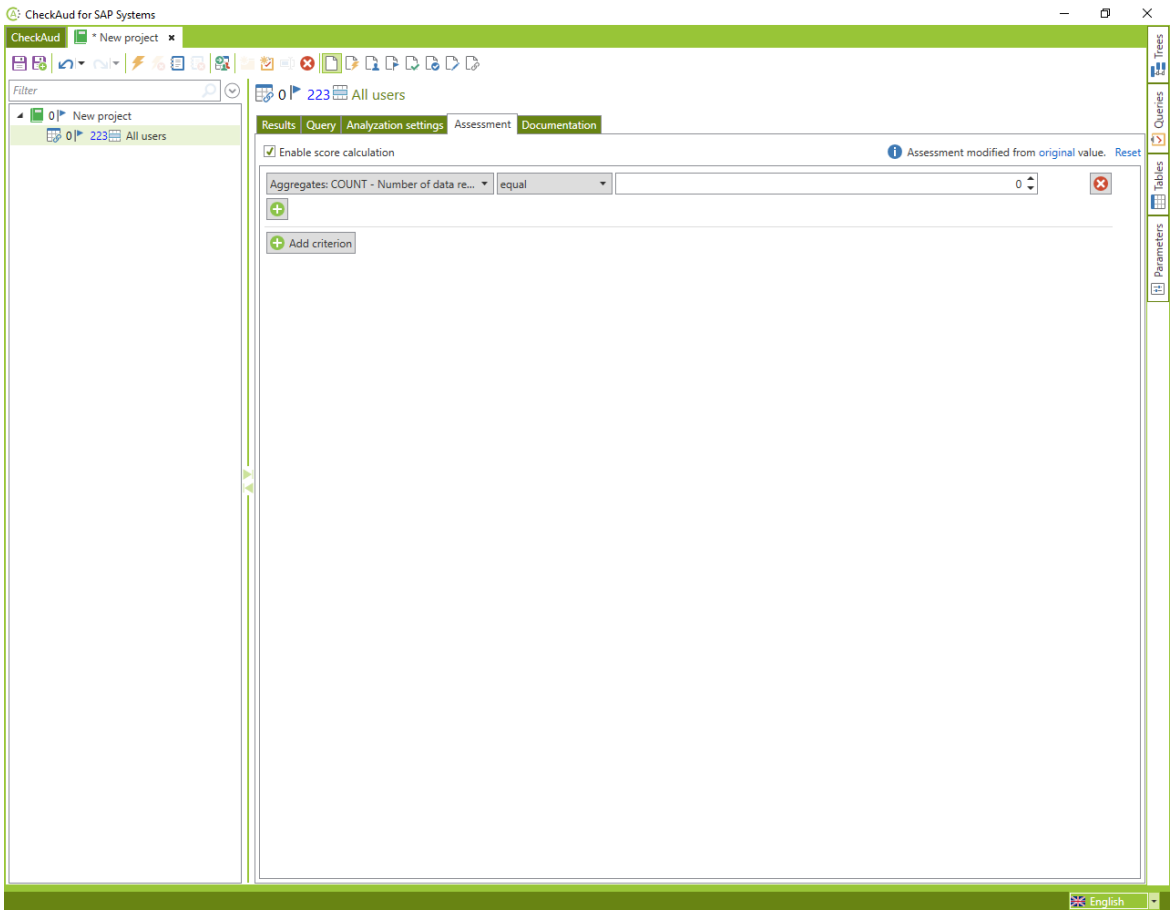



**Figure 349 - Creating a table query assessment**

For a table query with an assessment, you can calculate a score that is subsequently included in the score calculation for the project. However, this is not compulsory. If you want to calculate the score, you must set the relevant indicator:

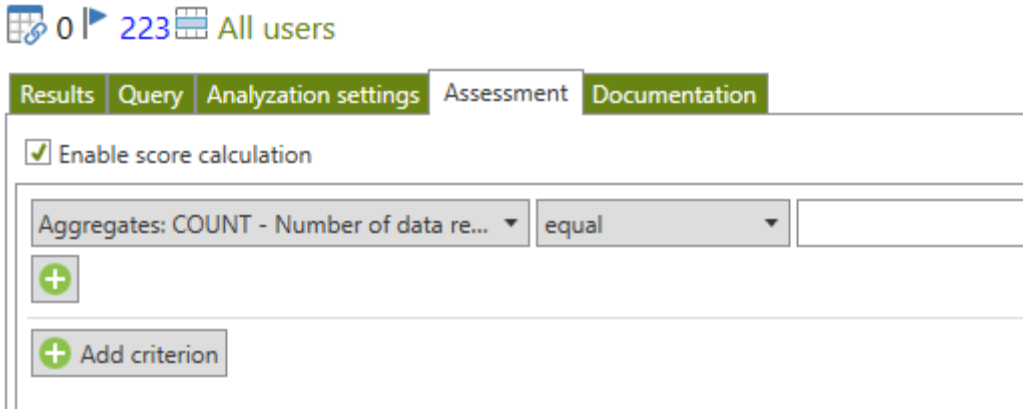
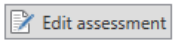



**Figure 350 - Activating the score calculation**

Predefined table queries are delivered with a preset assessment. However, you will naturally need to adjust the assessment to meet your own requirements on occasion. You can do so without having to remove the reference to this table query. You can use the 

button to do this.

# V - 5 Parameter values

## V - 5.1 Predefined parameter queries

The predefined parameter queries are the presets for the DSAG guidelines for SAP ERP 6.0 and the IBS Best Practice presets. The predefined parameter queries contain preset values for the stored parameters. These values are determined from the specified snapshot during the project analysis and compared with the presets.

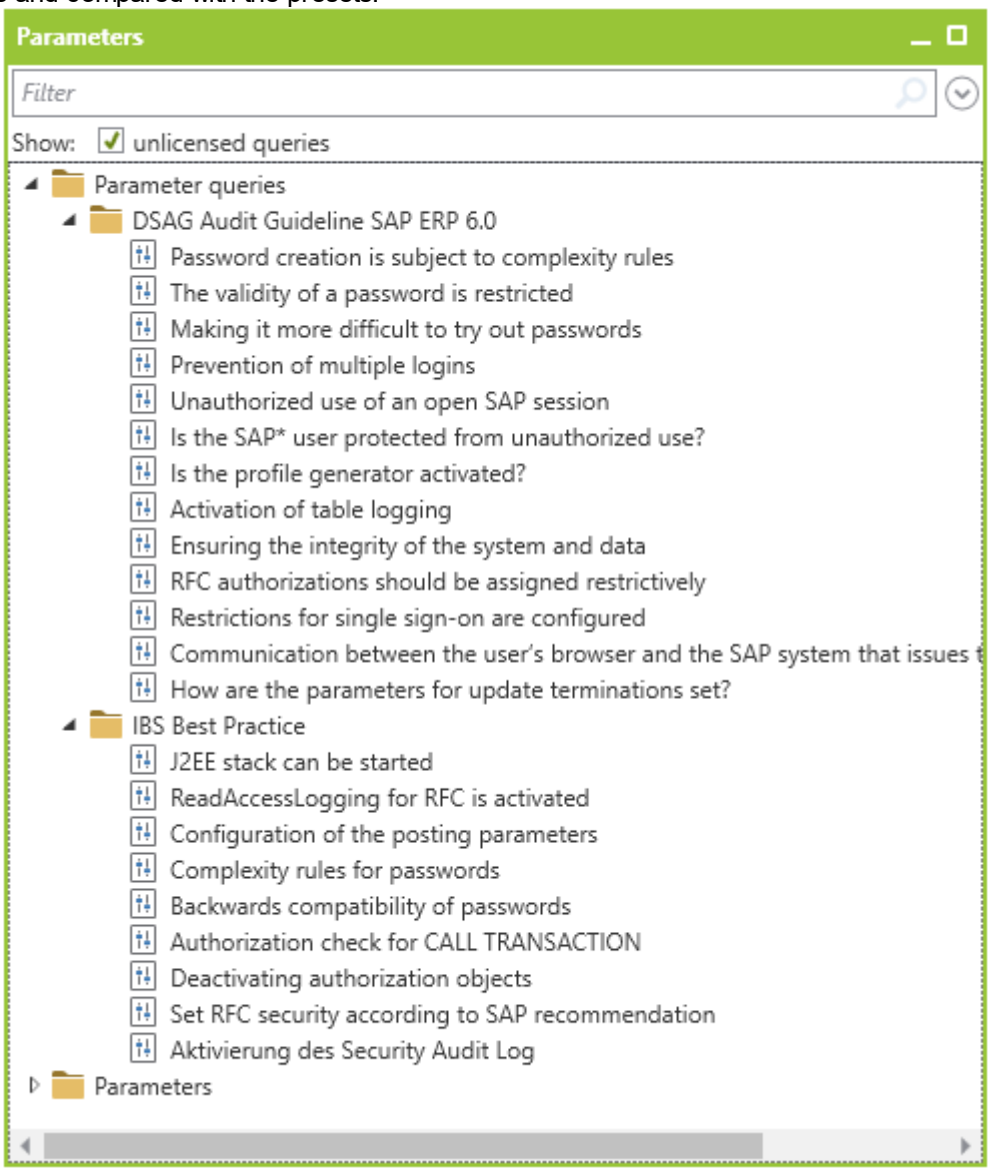



**Figure 351 - Predefined parameter queries**

You can use the filter functions to search for parameter groups or parameter queries that contain the parameter groups.

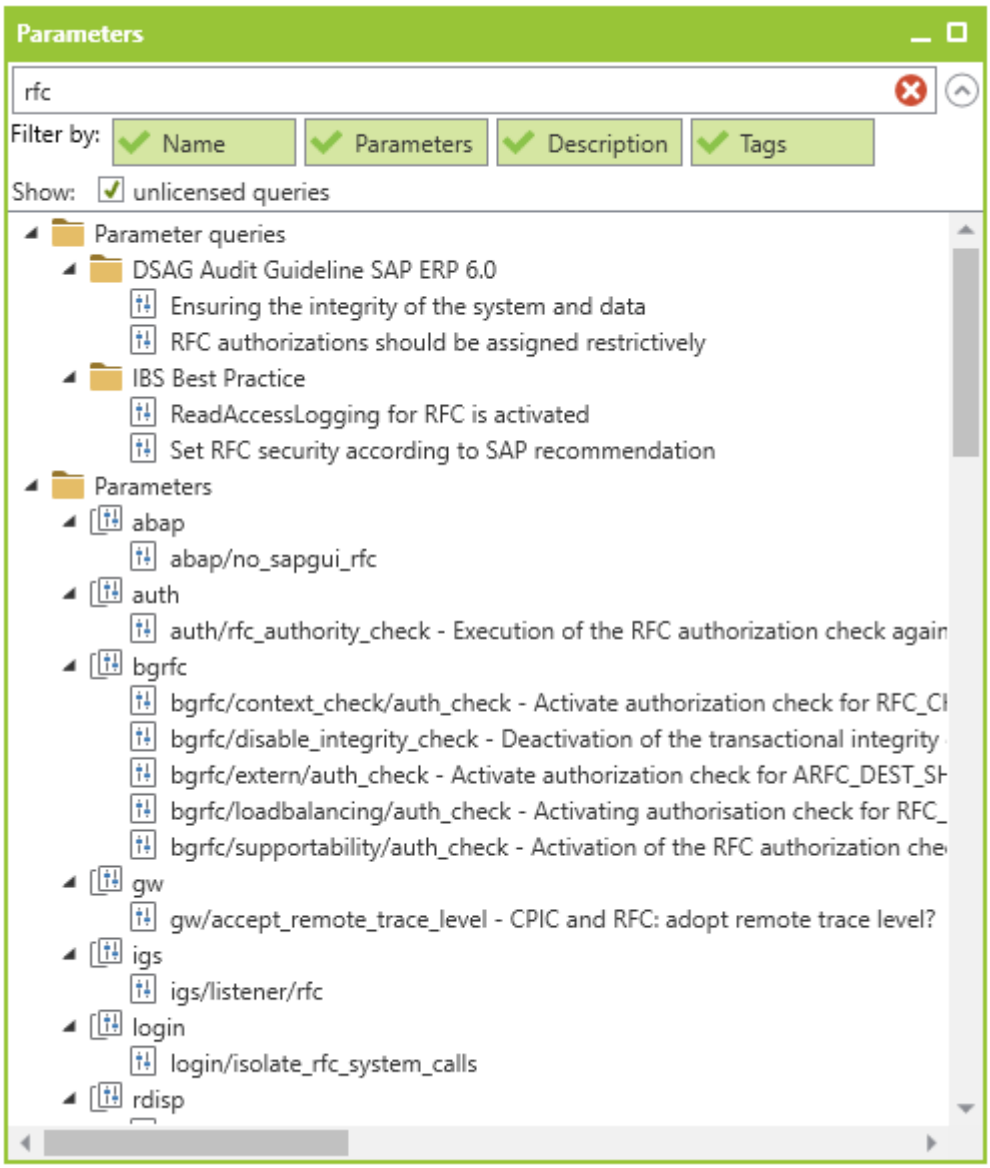
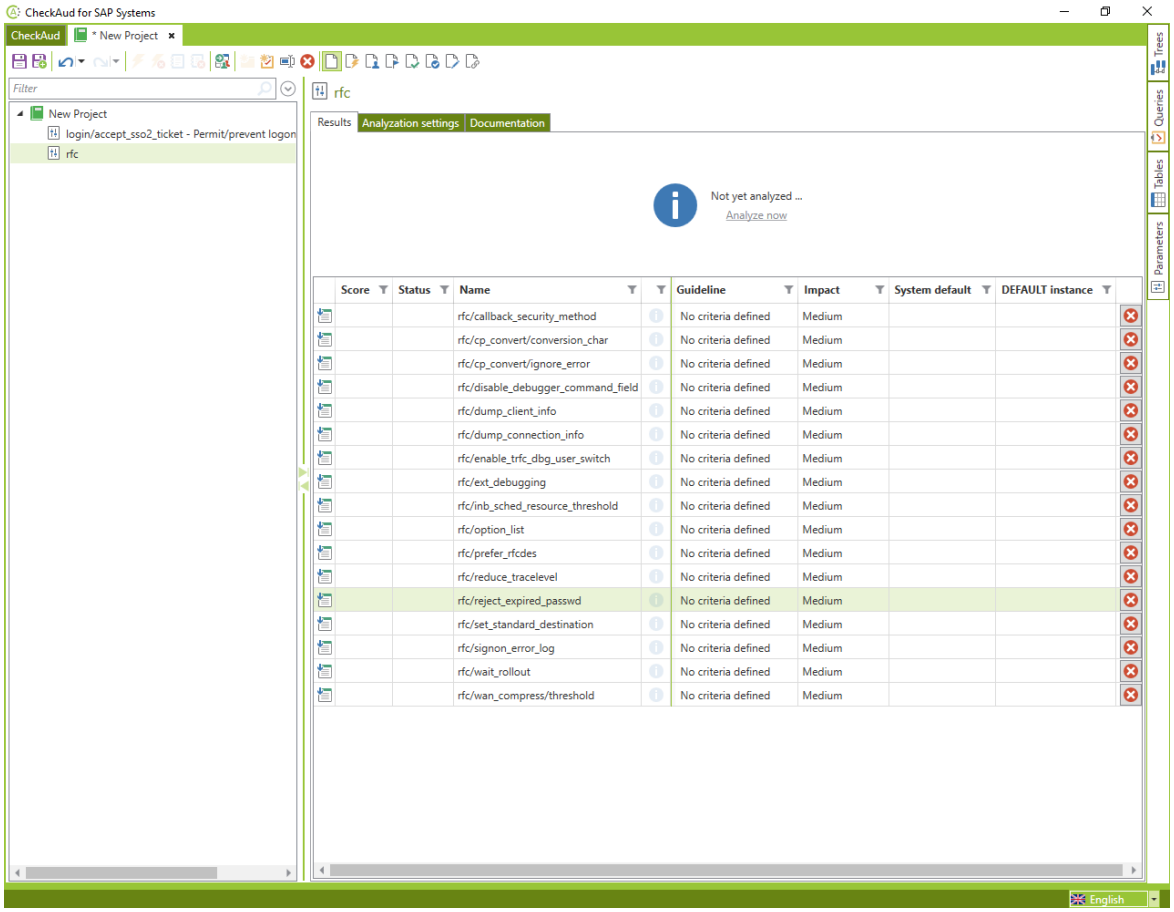



**Figure 352 - Searching for parameters**

## V - 5.2 Creating own parameter queries

You add parameters using drag and drop. Both individual parameter values and parameter groups can be queried. To add parameter groups, you select the relevant parameters from the *Parameters* toolbox and add them to the project tree using drag and drop. After the analysis, all of the parameters in the group are available.

You can use the -icon to delete parameters that are not required from the parameter group.




| Score | Status | Name | Guideline | Impact | System default | DEFAULT instance |
|---|---|---|---|---|---|---|
| | | rfc/callback_security_method | No criteria defined | Medium | | |
| | | rfc/cp_convert/conversion_char | No criteria defined | Medium | | |
| | | rfc/cp_convert/ignore_error | No criteria defined | Medium | | |
| | | rfc/disable_debugger_command_field | No criteria defined | Medium | | |
| | | rfc/dump_client_info | No criteria defined | Medium | | |
| | | rfc/dump_connection_info | No criteria defined | Medium | | |
| | | rfc/enable_trfc_dbg_user_switch | No criteria defined | Medium | | |
| | | rfc/ext_debugging | No criteria defined | Medium | | |
| | | rfc/inb_sched_resource_threshold | No criteria defined | Medium | | |
| | | rfc/option_list | No criteria defined | Medium | | |
| | | rfc/prefer_rfcdes | No criteria defined | Medium | | |
| | | rfc/reduce_tracelevel | No criteria defined | Medium | | |
| | | rfc/reject_expired_passwd | No criteria defined | Medium | | |
| | | rfc/set_standard_destination | No criteria defined | Medium | | |
| | | rfc/signon_error_log | No criteria defined | Medium | | |
| | | rfc/wait_rollout | No criteria defined | Medium | | |
| | | rfc/wan_compress/threshold | No criteria defined | Medium | | |

**Figure 353 - Parameter group list**

## V - 5.3 Defining presets and impact

You define your own presets using the  icon. To do so, you add the desired parameter to the project tree and select it. You can now define the effect and the criteria for the parameter.

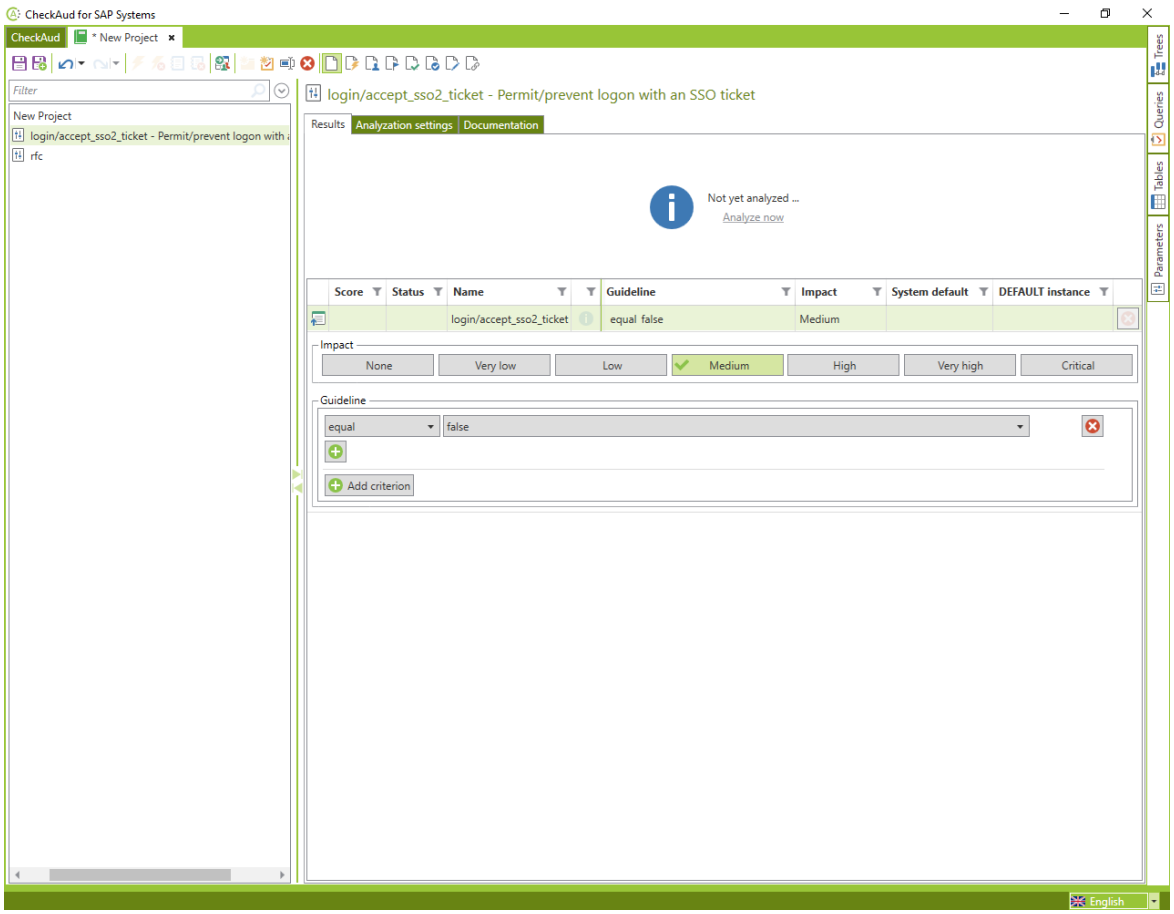



**Figure 354 - Creating presets for the parameter evaluation**

The defined impact has an influence on the analysis score for the parameter query. The higher the defined risk, the stronger the defined impact on the analysis score.

**Note:** Predefined parameter queries are supplied with a predefined impact that can be changed by removing the reference.

You can use the *Add criterion* button to add the operator for comparing the parameter value to the specification. The following operators are available:

- Equal
- Not equal to
- Less than
- Less than or equal to
- Greater than
- Greater than or equal to

If necessary, the operators can include an AND or OR link if more than one default value is assigned to the relevant parameter.

You can also define the impact (that is, the damaging impact to be expected if the target specification is not fulfilled). The same toolbar from the authorization query can be used to do so:

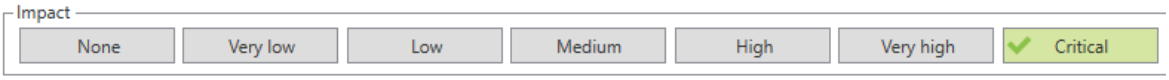



**Figure 355 - Configuring the impact**

This setting has an effect on the calculation of the score for the parameter query.

# Chapter VI - Automation

# VI Automation

Automation allows individual processes such as scanning the SAP systems, importing snapshots and analyzing and exporting projects to be performed automatically. Configuring it only takes a few steps.

## VI - 1 Command line module

The CheckAud command line module was developed for the completely automated run of a check, starting with the scan and followed by the export. A CheckAud analysis project must be created beforehand to use this tool. This analysis project must be preconfigured because no configuration is possible during the automated run.

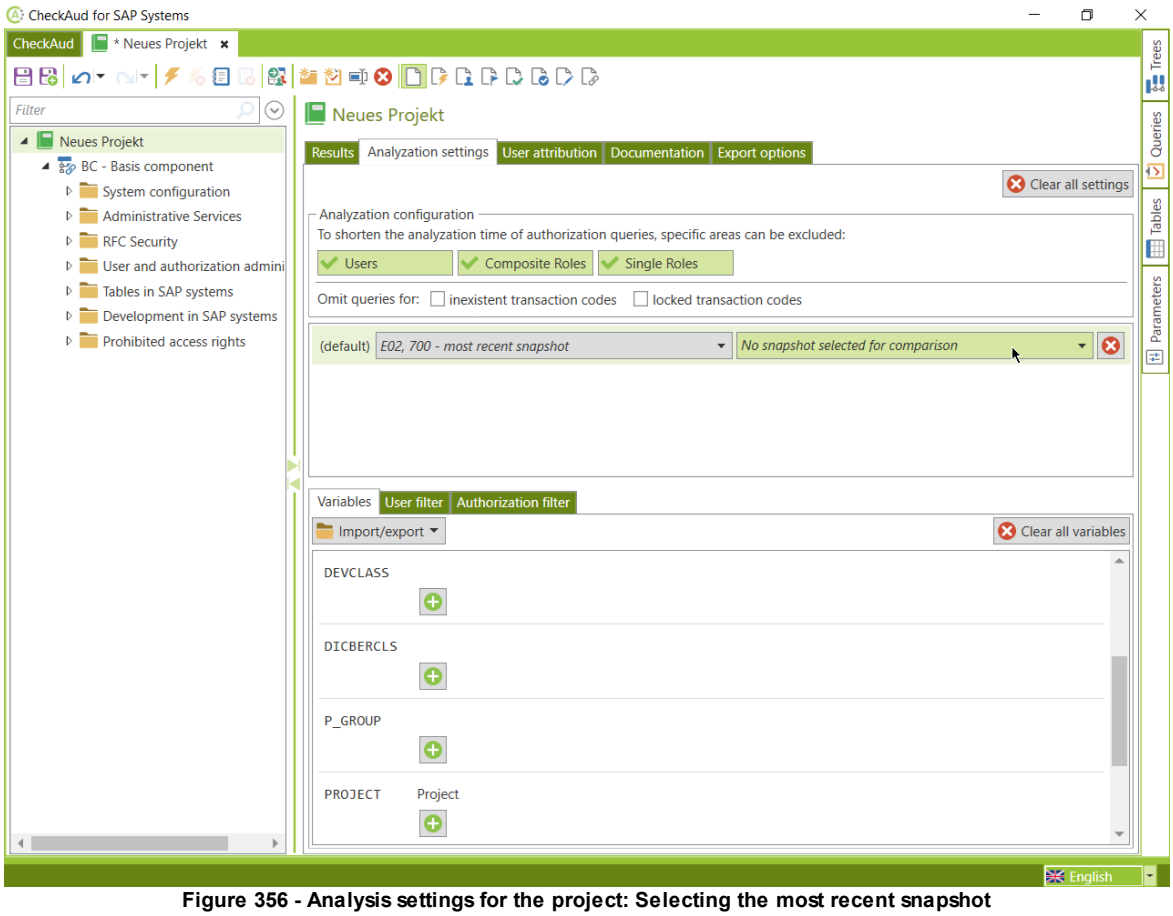



**Figure 356 - Analysis settings for the project: Selecting the most recent snapshot**

In the project, it is very important that System *name* – *most recent snapshot* is selected under the analysis settings for the snapshot. If this is not the case, an abortion of the analysis will occur during the analyzing process.

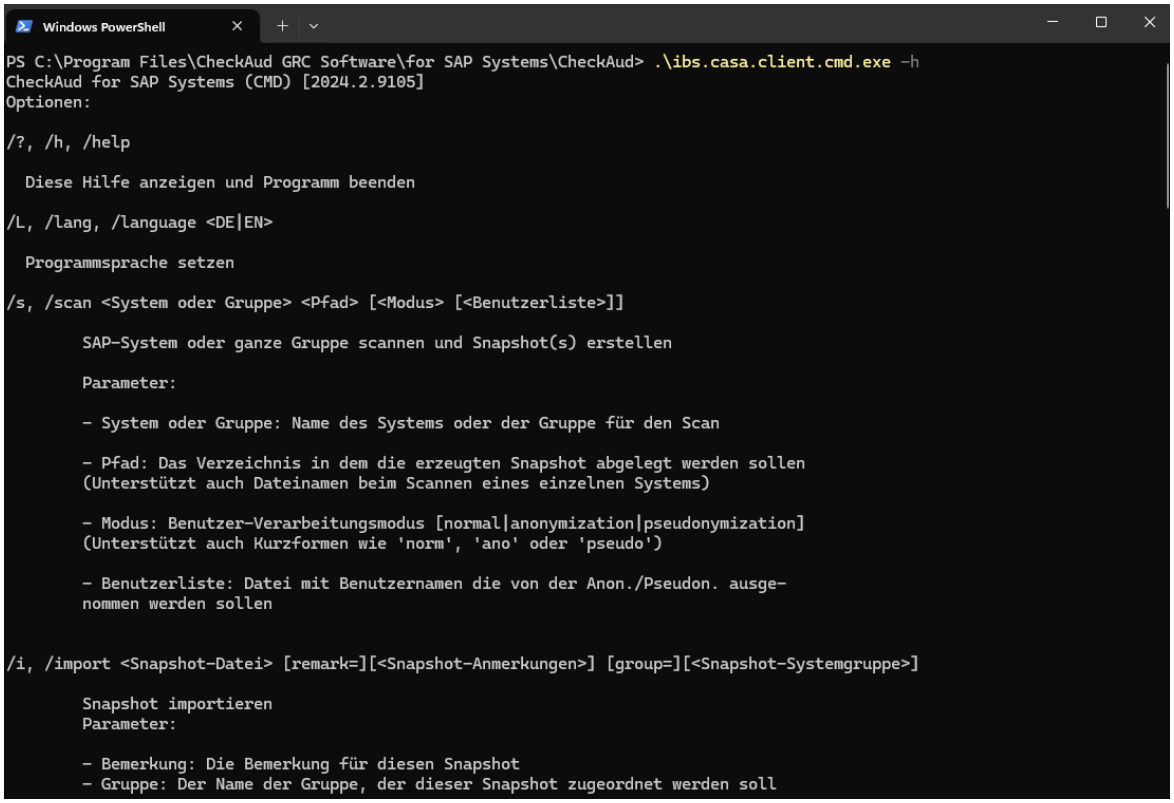



**Figure 357 - Example of calling a command line**

To call up the CheckAud command line module, you must specify the complete path of ibs.casa.client.cmd.exe in the command line. The quotation marks have to be observed here; otherwise, errors will occur due to blank spaces in the file path. In the standard installation of CheckAud, the file path is:

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
```

**Hinweis:** if only the scan module ist installed, it can be also startet via command line for automated scans:

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.scan.cmd.exe"
```

## VI - 2 Description of the function

The command line can be used to start CheckAud with various control parameters. These parameters are explained below:

`/?, -h, /h, /help`
This function can be used to call the module help, where the individual functions are listed.

`/L /lang[uage] [DE|EN]`
This function changes the language. You can enter either DE or EN. The set system language is used as the default.

`/s /scan <system|group> <path> [<mode> [<userlist>]]`
A snapshot of a system is then created. The system parameter must correspond to the title already maintained in CheckScan in the description of the SAP system to be scanned. The group parameter

represents the group maintained beforehand in CheckScan. Instead of an individual system scan, a group of systems can be scanned. The path under which the snapshot is saved is specified In the second parameter path. Individual snapshots can be provided with individual names. If a name is not explicitly assigned, CheckScan creates the name from the system ID, client, date and time. Groups automatically receive the name from the system ID, client, date and time. It is not possible to assign individual names with groups. The third and fourth parameters are optional. If necessary, the snapshot can be anonymized or pseudonymized. If the parameter is not set, the snapshot automatically receives the user mode normal. A user list can be loaded with the fourth parameter. Thanks to the user list, the names stored in the list are no longer anonymous or pseudonymous.

**Example: Creating a snapshot with a specified name:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/s "IBS E02" "C:\users\BENUTZER\desktop\IBS_E02.casnapshot"
```

**Example: Scanning a group:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/s "Gruppename" "C:\users\BENUTZER\desktop"
```

**Example: Creating a pseudonymized snapshot:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/s "IBS E02" "C:\users\BENUTZER\desktop\IBS_E02.casnapshot" pseudonymize
```

**Example: Creating a snapshot, when only the scan module is installed and used:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.scan.cmd.exe"
/s "IBS E02" "C:\users\BENUTZER\desktop\IBS_E02.casnapshot"
```

When pseudonymization is activated, the Excel list with the comparison of pseudonymized and plain text names is created at the same time in the target snapshot directory. This is not the case when using anonymization.

The following user mode spellings are available:

Anonymization user mode:

- `Ano`,
- `anonymize` or `anonymise`,
- `anonymization` or `anonymisation`

Pseudonymization user mode:

- `pseudo`,
- `pseudonymize` or `pseudonymise`,
- `pseudonymization` or `pseudonymisation`

Normal user mode:

- `normal`

**Example: Creating a pseudonymized snapshot with a user list:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/s "IBS E02" "C:\users\USER\desktop\IBS_E02.casnapshot"
pseudonymize "C:\users\USER\desktop\UserList.txt"
```

**Example: Basic system scan:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/s "IBS E02" "C:\users\USER\desktop\IBS_E02.casnapshot"
```

`/i, /import <Snapshot file> [<snapshot remark>]`

This scan is used to import the snapshot created previously to CheckAud to start the analysis. The file name of the snapshot must be specified as a parameter. Furthermory it is optional to set a remark for this snapshot during the import.

**Example Importing the scan to CheckAud:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/i "C:\users\USER\desktop\IBS_E02.casnapshot"
```

`/i, /import <Snapshot file> <Remark>`

With the option <remark> a remark can be added to the snapshot during the import process.

**Example for importing a snapshot with remarks**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/i "C:\users\BENUTZER\desktop\IBS_E02.casnapshot" remark="This is a remark"
```

`/i, /import <Snapshot file> <Group>`

With the option <Group> the snapshot to be imported will be assigned to a specified snapshot goup.

**Example for importing a snapshot and assigning this snapshot to a group**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/i "C:\users\BENUTZER\desktop\IBS_E02.casnapshot" group="New group"
```

`/l, /load <project>`

In this function, you specify the exact path for loading a project created previously.

**Example: Loading a project:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/l "C:\Users\USER\Desktop\Projektname.caproject"
```

`/reset (compare|variables|userfilter|authfilter|userattr)`

Deactivates the snapshot comparison and deletes the defined variables, user filters, authorization filters or user assignments. You configure all the settings directly on the project node. The selection of a different node is not currently supported. We recommend that you execute the function /reset when changing variables, user filters, authorization filters or user assignments.

**Example: Deleting variable sets:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/reset variables
```

`/set snapshot <system ID> <client>`

This function allows you to switch snapshots in the batch file. When you specify the system ID and client, the most recent snapshot of the relevant system is loaded. If a comparison is configured in the analysis settings in the project, it is retained only if the new snapshot originates from the same system/client combination. In all other cases, the comparison is deactivated by changing the snapshot.

**Example: Loading a different snapshot:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/set snapshot IB3 800
```

`/set compare (second|least)`

This parameter can be used to configure the comparison of two snapshots. When doing so, you select the second newest (“second”) or oldest (“least”) snapshot for the system/client combination that was configured as the target snapshot. When configuring the comparison, you must always set the relevant target snapshot first before using this parameter to select the desired comparison snapshot.

**Example: Activating the comparison with the second newest snapshot of the current selected system:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/set compare second
```

`/setall snapshot [<group>] <system ID> <client>`

This parameter sets the most recent snapshot of the specified system/mandant or system/database combination not only at the project root level, but also on all elements where analysis settings inheritance has been disabled.

```
/setall compare [ABAP|HANADB] (second|least)
```

This parameter sets a snapshot comparison not only on the project root, but also on all project elements where the inheritance of the analysis settings has been disabled.
To configure the comparison, the respective target snapshot must always be set first. If the project only targets ABAP or HANA DB, the type of the target system is automatically detected, otherwise the target system must be specified after /setall compare. Then it is defined whether the comparison should be made with the second most recent ("second") or oldest ("least") snapshot of the same system/mandant or system/database combination.

```
/resetall compare
```

This parameter resets a snapshot comparison not only on the project root, but also on all project elements where the analysis settings inheritance has been disabled.

```
/set (variables|userfilter|authfilter|userattr) <file>
```
This function is provided so that you can change the variable set, user filter, authorization filter or user assignment in a project at a later stage. You can also use it to perform multiple evaluations with various filters. You must ensure that the correct file type is selected when setting the filter.

variables: Variable set (.cavariables)
userfilter: User filter (.causerfilter)
authfilter: Authorization filter (.caauthfilter)
userattr: User assignment (.causerattribution | .xls/.xlsx (if it is a compatible user authorization matrix))

**Example: Loading variable sets:**
```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/set variables C:\CheckAud-Variablen.cavariables
```

```
/a, /analyze
```
You can use this function to analyze a project that was loaded beforehand. This option has been supplemented by the optional parameter abort= with the values never, critical and all.
This can be used to control which errors cause the analysis to be aborted:

- none = all errors are ignored and the analysis is continued (this is the default behavior)
- critical = only critical errors (such as “Out of memory”) cause the analysis to be aborted; missing tables (sets) are ignored
- all = all errors cause the analysis to be aborted, including missing tables (sets)

```
/export <export path/file>
```
This function specifies the file path to which the analysis results are exported. Please note: If the path specified ends with “.htm” or “.html,” it will be considered a file name. In all other cases, the path will be considered a specification of a directory, the directory will be created if necessary and a unique file name will be generated. The format of the generated file name is “<project name>_<export time>.html". The export time is written in the “YYYYMMDD_HHMMSS” format.

**Example of an analysis that is then exported:**
```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/load "C:\users\USER\BeispielProjekt.caproject"
/a
/export "c:\users\USER\desktop\test.html"
```

`/p, /progess`
With this function, one of the other subprocesses can be monitored in more detail if the standard output of this function is to be transferred to a log file. This is used for error processing, or traceability of the process in question.

`/delete (<system ID>|*) (<client>|*) [age]`
Snapshots that are no longer required can be completely deleted from the CheckAud database using this function. You use the “system ID” parameter to select the desired system. If you specify “*” instead of an individual system ID, all the systems in the CheckAud database are selected. You can use the “client” parameter to select individual clients for deletion. You can also use the “*” to select all the clients in the SAP system simultaneously here. The “age” parameter specifies the maximum age that the snapshot is permitted to be. Snapshots that exceed the specified age are deleted from the database. The age can be defined as integers in the following time units:

d for days
w for weeks
m for months
y for years

If no time period is defined, all the snapshots of the specified SAP system are deleted.

**Example: Deleting individual client 800 snapshots that are more than 2 years old from the IB1 SAP system:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/delete IB1 800 2y
```

**Example: Deleting all snapshots from the CheckAud database:**

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/delete * *
```

Individual snapshots or whole system IDs that have been provided with write protection cannot be deleted from the database. The snapshots or system IDs can only be deleted once the write protection is removed.

**Note:** When creating these processes, observe the order of the individual parameters because the command line module processes the individual commands one after the other. The “/L” language setting and process progress indicator (/p) must be defined at the beginning because the language setting and process progress can no longer be taken into consideration at the end of the command line. The basic settings from the CheckAud graphical user interface are used.

**In addition, we recommend closing the CheckAud and CheckScan programs when using automation.**

An example is listed below, in order to illustrate the functionality.

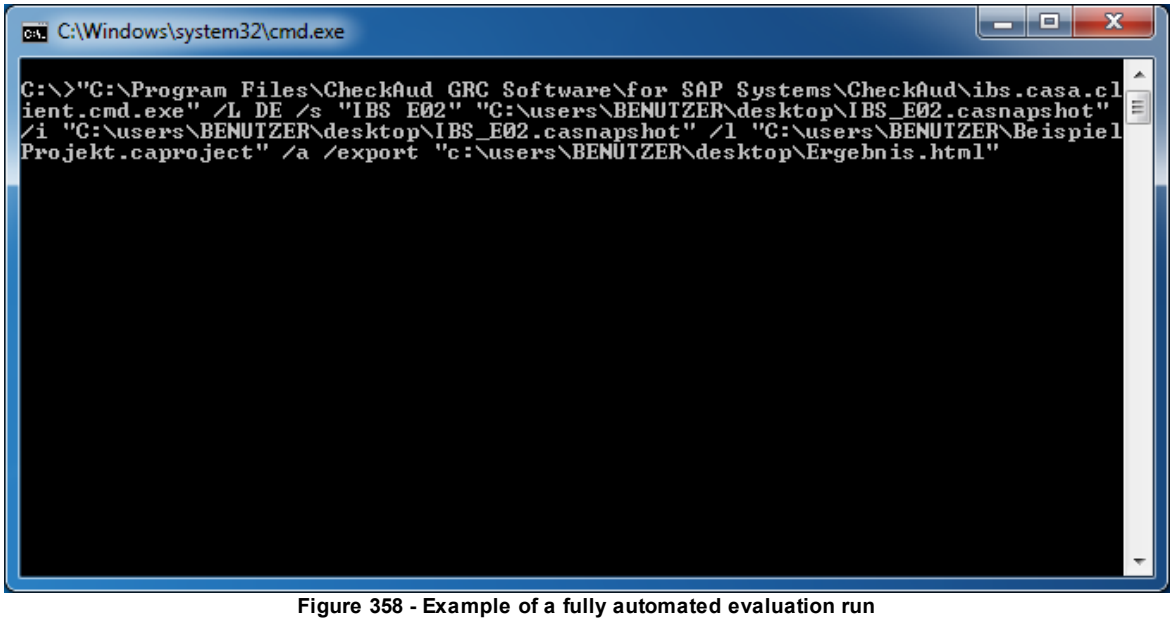



**Figure 358 - Example of a fully automated evaluation run**

The following steps are performed in the example here:

- Changing the language to English (/L)
- Scanning the SAP system IBS E02 and then saving the snapshot (/s)
- Importing the created snapshot (/i)
- Loading a created project (/l)
- Analyzing the project (/a)
- Exporting the analysis results (/export)

Example in text form:

```
"C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckAud\ibs.casa.client.cmd.exe"
/L DE
/s "IBS E02" "C:\users\USER\desktop\IBS_E02.casnapshot"
/i "C:\users\USER\desktop\IBS_E02.casnapshot"
/l "C:\users\USER\BeispielProjekt.caproject"
/a
/export "c:\users\USER\desktop\Ergebnis.html"
```

**General note on automation with umlauts::**
If umlauts are used in the batch file, an error message is issued when performing automation in the incorrect code page. We recommend that you do not use umlauts in the batch file or take one of the following hints into consideration.

*1. Saving a file with the correct code page*
The batch file must be created with an editor that supports switching between different code pages (for example, UltraEdit, Notepad++, etc.). When you save, you must then select CP850 or a suitable equivalent. Umlauts will then work without issue.

*2. Switching code page in the batch*
You could change the code page to the code page that was used during editing directly at the start of the batch file. If the batch file was created using Notepad in a western European language, the first command would have to be chcp 1252. However, this has the side effect that the umlauts are now displayed as unwanted special characters in the command line (both the umlauts contained in the batch and the umlauts output by CheckAud).

# VI - 3 Planning scans using a batch file

In Windows, there is a function in the Task Scheduler that can be used to perform certain tasks in a recurring rhythm in the background. This creates a simplified working method and relieves the SAP system because the start of the scans can be set to times when the utilization in the SAP system is low.

## VI - 3.1 Task preparation

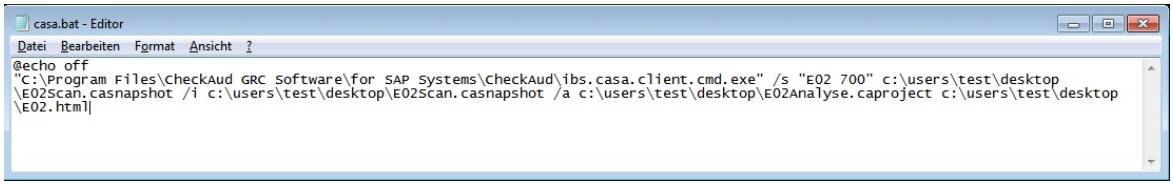



**Figure 359 - Executable batch file**

A complete run of a check can be performed with this batch file, as shown at the start of this chapter. Make sure that the relevant name assignment and path specification are formed correctly. Furthermore, a project must be created prior to planning and connected to a snapshot so that the task planning can provide a successful result. It should be noted here that the project can of course be adapted to other queries afterwards. However, the naming of the project or snapshot should not vary.

## VI - 3.2 Task planning

To create a recurring task for regular scans and evaluations, you can use the Windows task scheduler. You can access this feature in your operating system control panel.

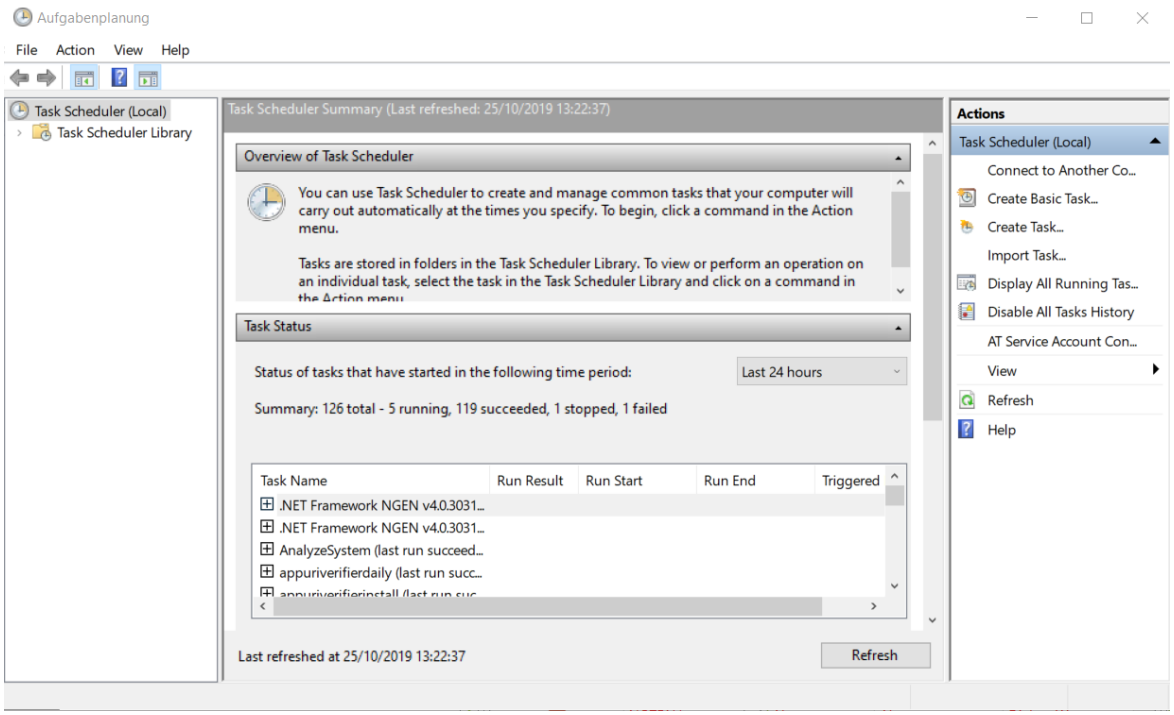



**Figure 360 - Scheduling a task**

In this window, any task can be defined and repeated in a set rhythm. To create a regular trigger of a system with subsequent analysis, the *create simple task* function must be selected in the right-hand action area.

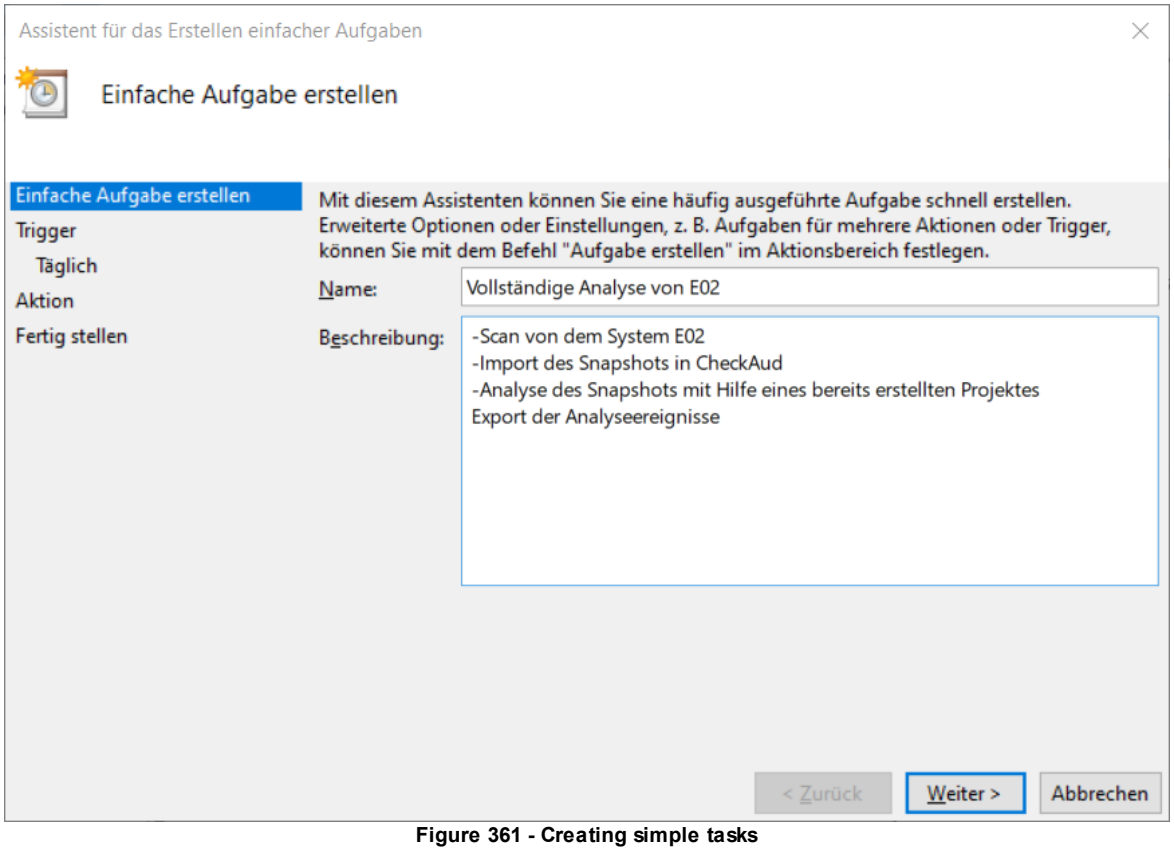



**Figure 361 - Creating simple tasks**

Defining a description is recommended, as an overview can then be created if several systems with different tasks are to be processed or if several employees have to interact with these tasks.

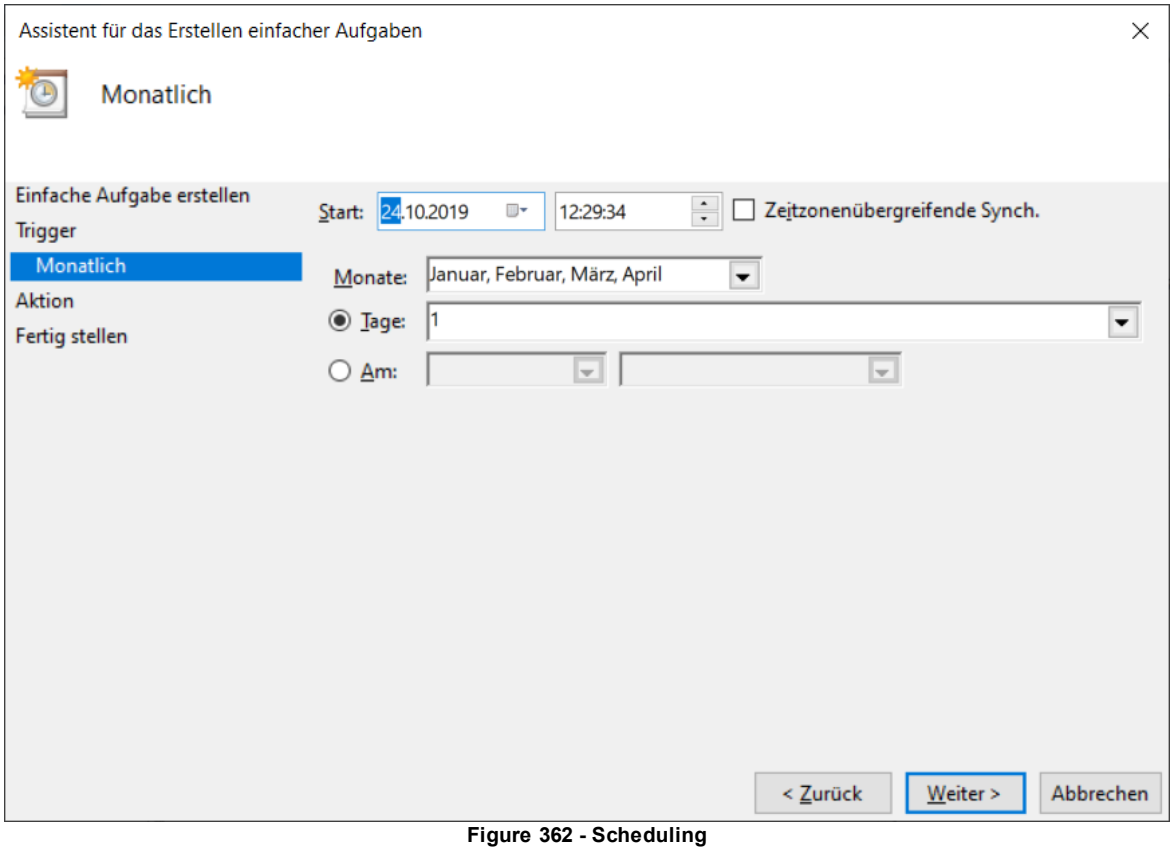



**Figure 362 - Scheduling**

The trigger for the task can be configured individually, depending on the type of inspection. The monthly inspection does not have to take place every month; instead, the month and the day of the month to be scanned can be defined.

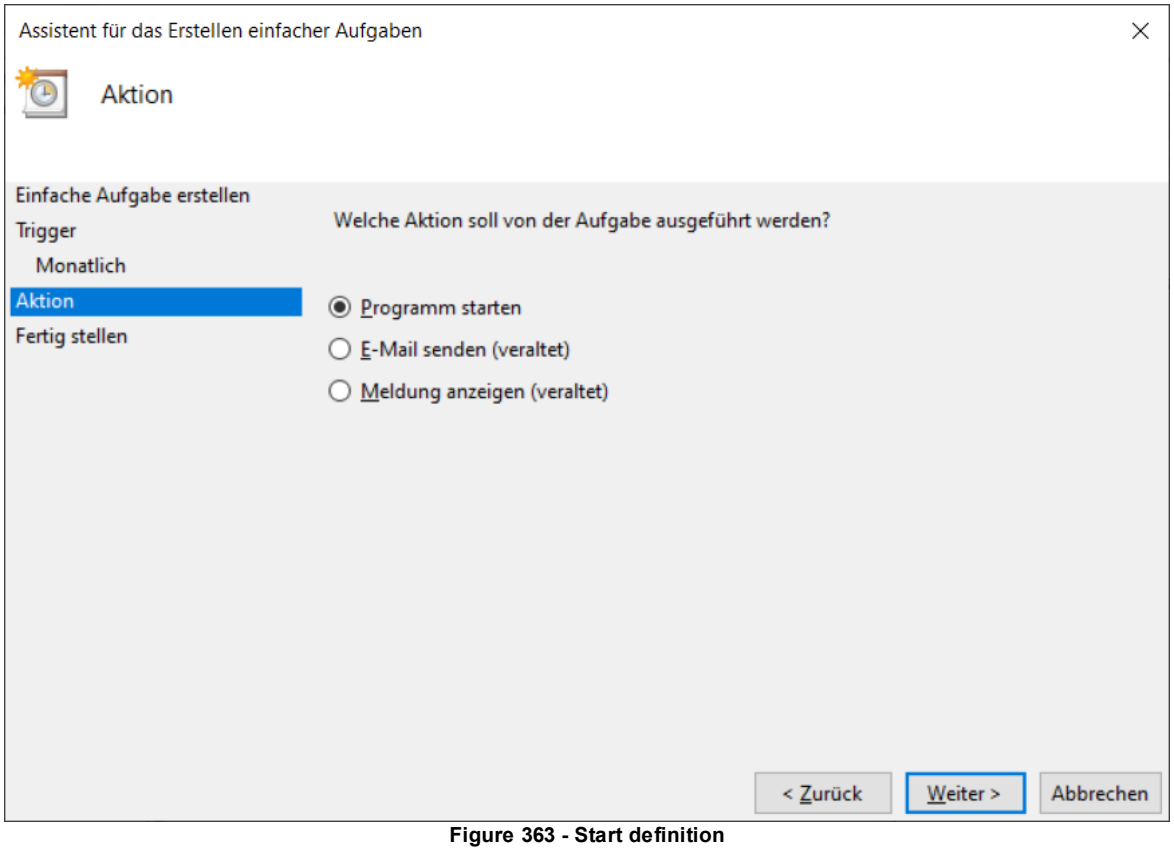



**Figure 363 - Start definition**

The “Start program” function must be chosen in the action selection because the batch format includes an executable file.

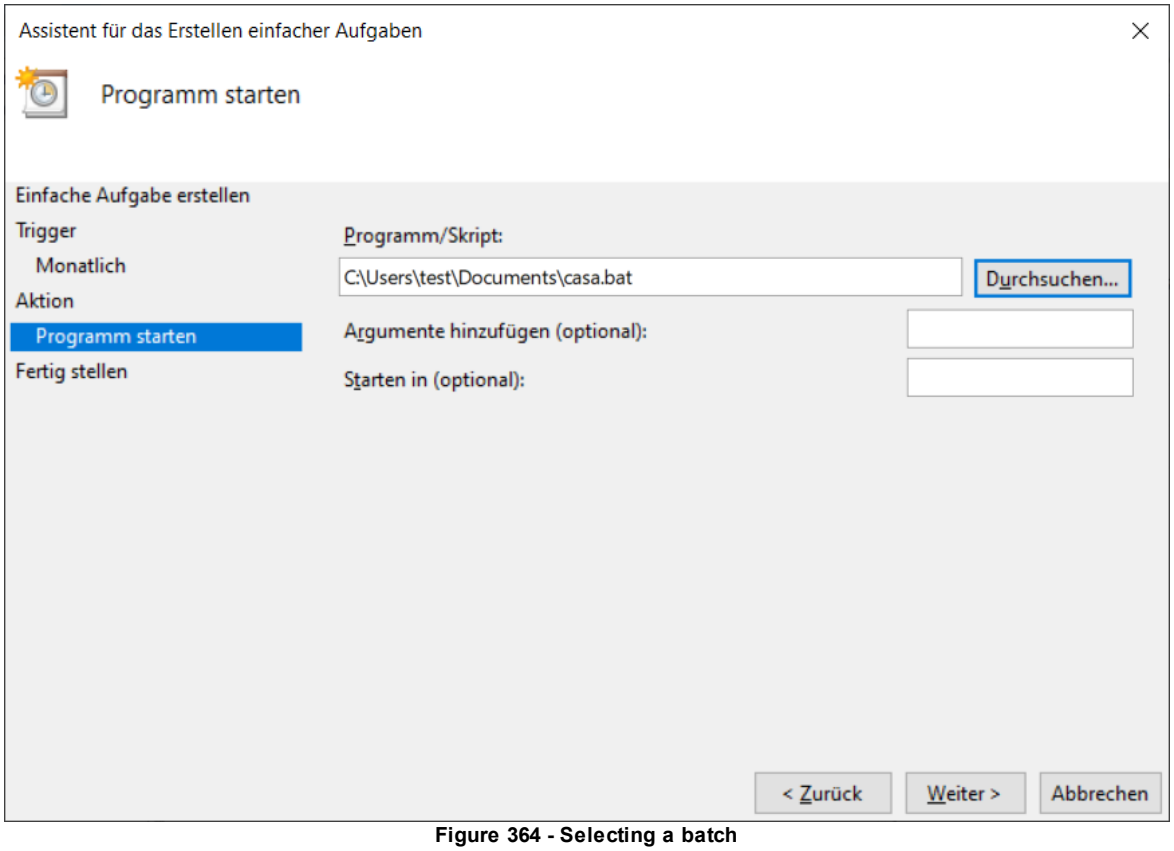



**Figure 364 - Selecting a batch**

The file path of the batch file that was configured beforehand is stored under *program/script*. This can be done using the browse button.

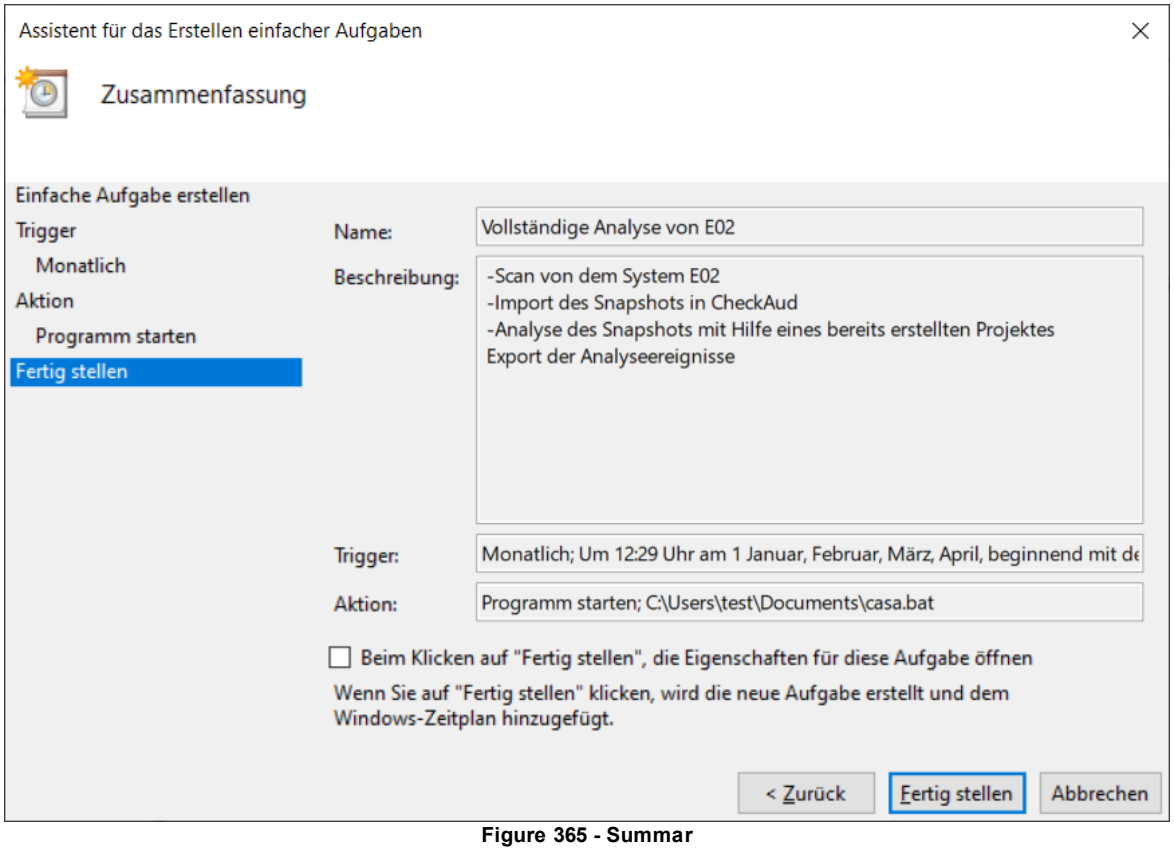



**Figure 365 - Summar**

In the summary, the settings should once again be thoroughly checked to see if they fulfill the requirements for a recurring inspection. As soon as the task has been completed, it is active and will always run if the trigger settings have been met.

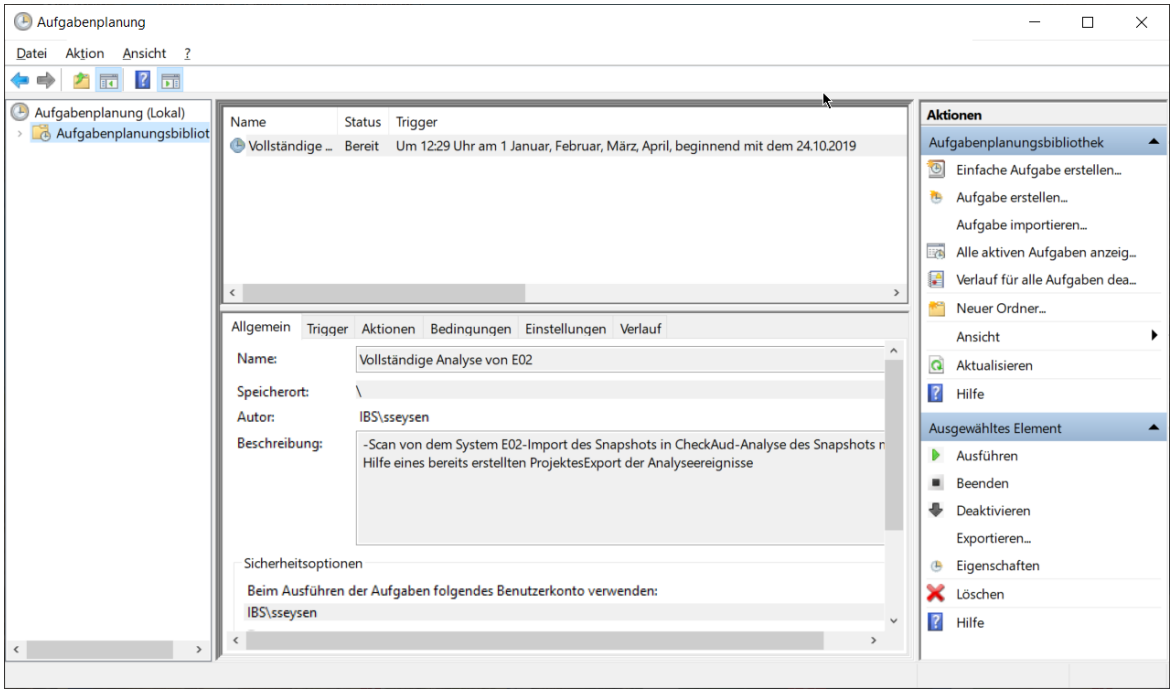



**Figure 366 - Overview of the created task**

All of the current user tasks can be seen in the task planner overview.

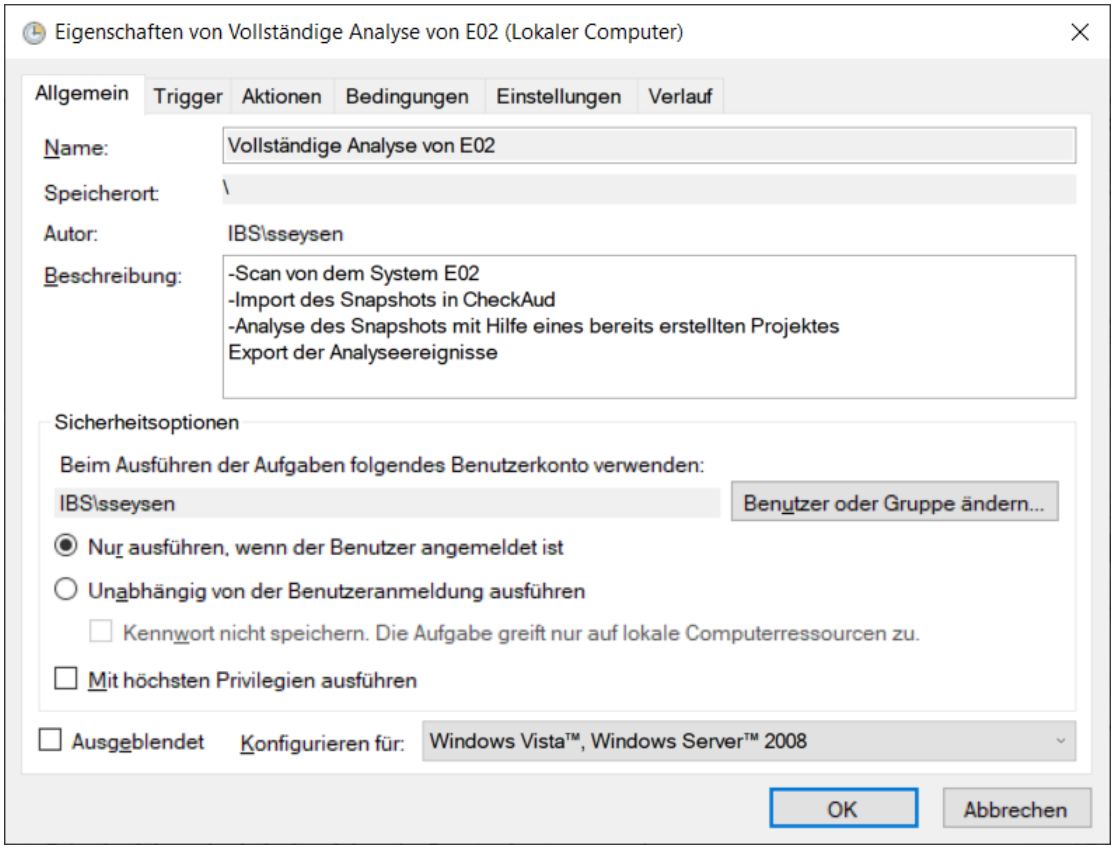



**Figure 367 - Activating a scan in the background**

To adapt tasks that have already been created, open the options menu by double-clicking on a task; adjustments can then be made to the task here. The command line appears when the current script is started. To stop this, you must select the option *Run independently of the user login*. This option allows the start of the batch file without the user having logged in to the system. Furthermore, the command line will also not appear on the screen. When you press the OK button, Windows requests the user data from which the task should be started..

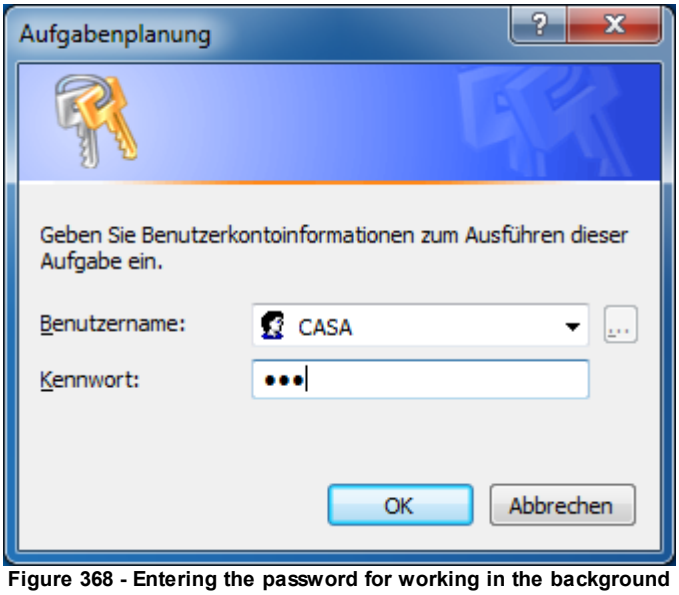



**Figure 368 - Entering the password for working in the background**

# Chapter VII - Logging of data handling

# VII Logging of data handling

CheckScan and CheckAud will create logs regarding the data handling to prove, what data and actions has been done with the scan and evaluation module. This might be necessary regarding data protection requirements

CheckAud creates event logs which can be checked with the event viewer of the operating system:

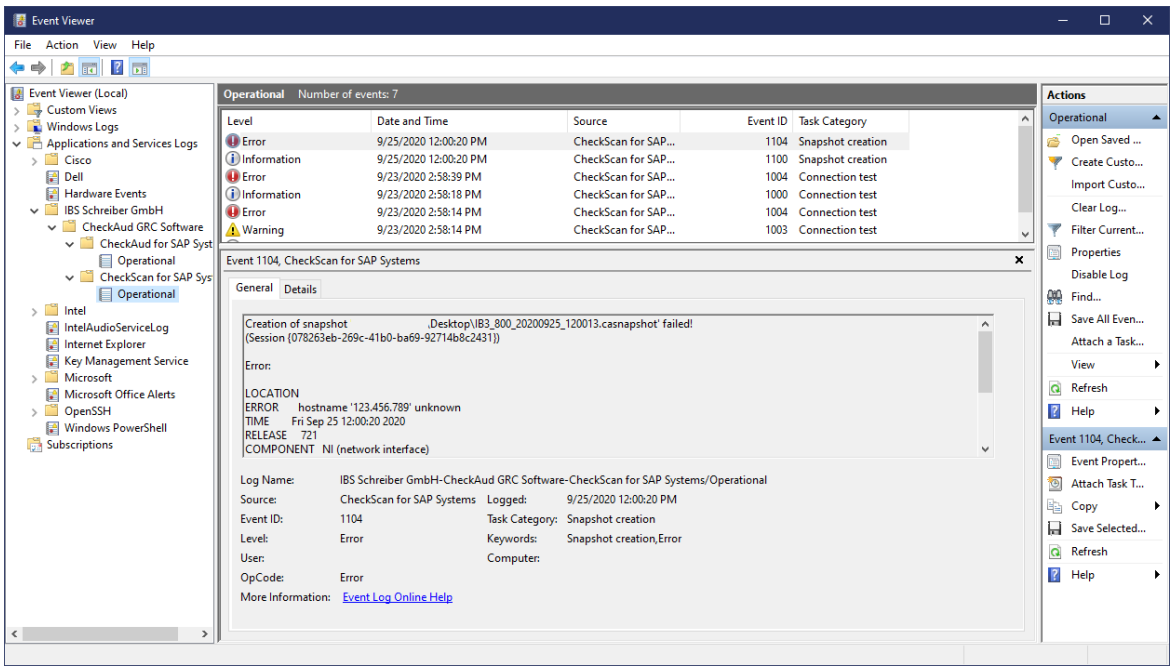



**Figure 369 - Event log CheckScan**

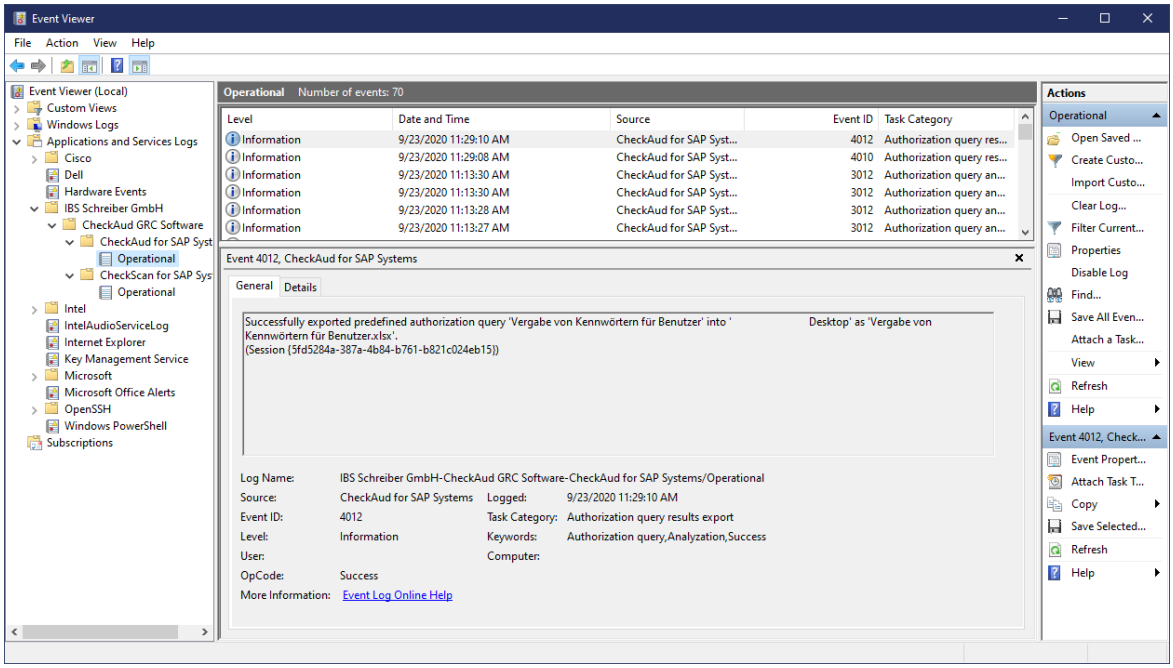



**Figure 370 - Event log CheckAud**

Detailed information to the messages of the event logging of CheckAud and CheckScan can be found in the separate *Data Protection Guide.*

# Chapter VIII - Technical Support & Updates

# VIII Technical Support & Updates

If you experience technical problems or have any questions about CheckAud, you can contact IBS Schreiber GmbH Support by phone or e-mail:

IBS Schreiber GmbH
Zirkusweg 1
20359 Hamburg, Germany
Telephone: +49 (0) 40 69 69 85-25
Fax: +49 (0) 40 69 69 58-80
E-mail: support@ibs-schreiber.de

Where possible, the following information must be provided:

- A brief description of the problem
- How the error came about
- Whether the error is reproducible
- The version of CheckAud® with which the error occurred
- The operating system that was being used

Additional screenshots of the error message or the process involved are always very helpful! IBS Schreiber GmbH Support will then log and process your support case. A response will be sent to you with the case number through the ticket system to confirm its receipt.

If program errors occur or the software crashes, you can view the log file and make it available to IBS Schreiber GmbH Support where required.
The log files for CheckAud can be viewed in the About CheckScan menu item in CheckScan and in the About CheckAud menu item in CheckAud.


**Figure 371 - Accessing the log files**

A log file is created each time that CheckScan and CheckAud are started. You can view the latest log file by clicking the Display current log file einsehenbutton. To view older log files, you can use the Open log directoy button. A Windows Explorer window opens when you click the link Open log directoy.

The log files for CheckScan are stored under the following name::
`casc_DATE_TIME.log`

Problems (e.g. authorization problems for the SAP user) when connecting CheckScan with the SAP system are stored under the following name:
`dev_nco_rfc.log`

The log files for CheckAud are stored under the following name:
`casa_DATUM_UHRZEIT.log`

The log files for CheckScan and CheckAud automation are stored under the following name:
`casd_DATUM_UHRZEIT.log`

It may be necessary to make these log files available to IBS Schreiber Support upon request in order to isolate the problems that occur more closely.

### Search for new updates

When opening the new version for the first time, this window appears automatically with the question for automatic update search. It can be activated, canceled or asked again later and does not mean installation yet:

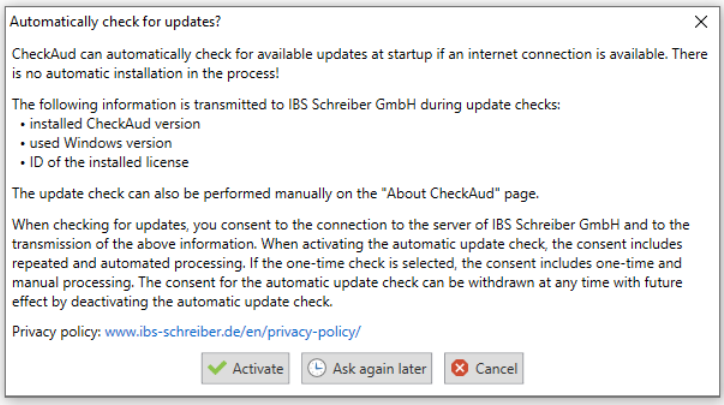



**Figure 372 - Search for new updates**

To ensure access to the update check, the client on which CheckScan / CheckAud is installed needs the ability to reach the URL https://transfer.ibs-schreiber.de/ via port 443.

### Settings for automatic updates

The automatic check for updates can be activated or deactivated in CheckAud as well as in CheckScan in Settings.

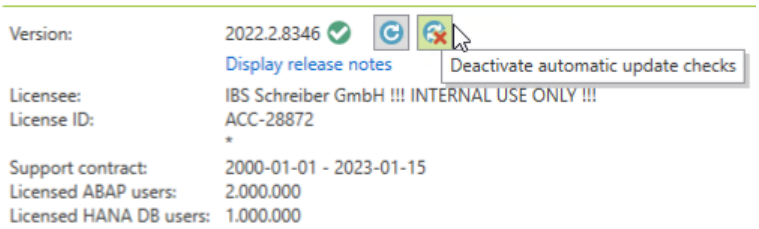



**Figure 373 - Disable automatic update check**

If the automatic update check is deactivated, it is possible to start an update check manually.

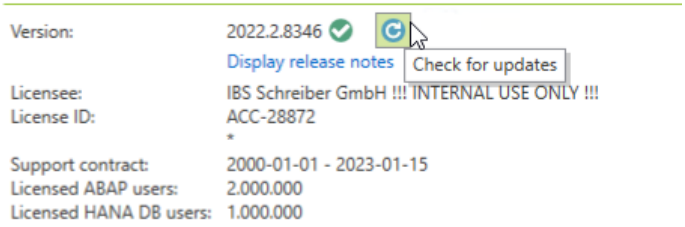



**Figure 374 - Manual update check**

After pressing the button a dialog window opens (see Figure 359 - Check for automatic updates) in which the automatic update check can be activated or a one-time check for updates can be performed.

### Proxy settings for automatic updates

If a proxy login is required during the update check, a note appears at the top of the window:

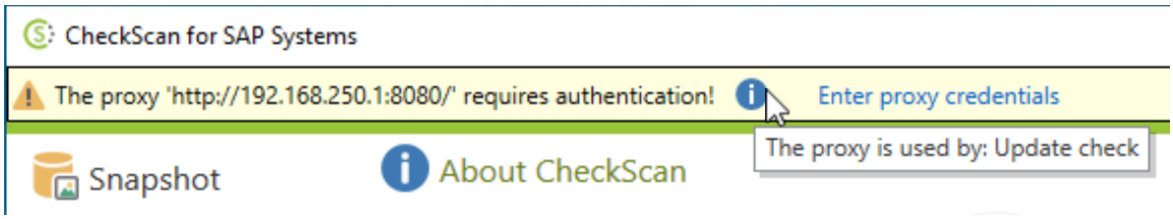



**Figure 375 - Proxy login data**

Via the link "Enter proxy credentials" the input window can be opened:

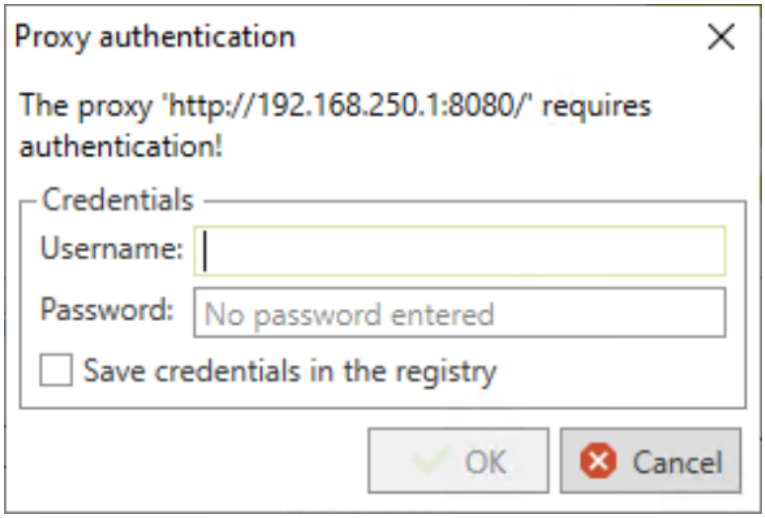



**Figure 376 - Proxy Authentication**

By default, the data is only kept in memory and is thus lost again when the program is closed.

If the option "Save credentials in registry" is selected, the entered data is additionally saved in the registry and automatically reloaded when the program is restarted. The storage takes place under HKCU, thus only for the Windows user currently logged in. The password is stored encrypted and can be decrypted only by this Windows user.

The data stored in the registry can be deleted again via the "Settings" page:

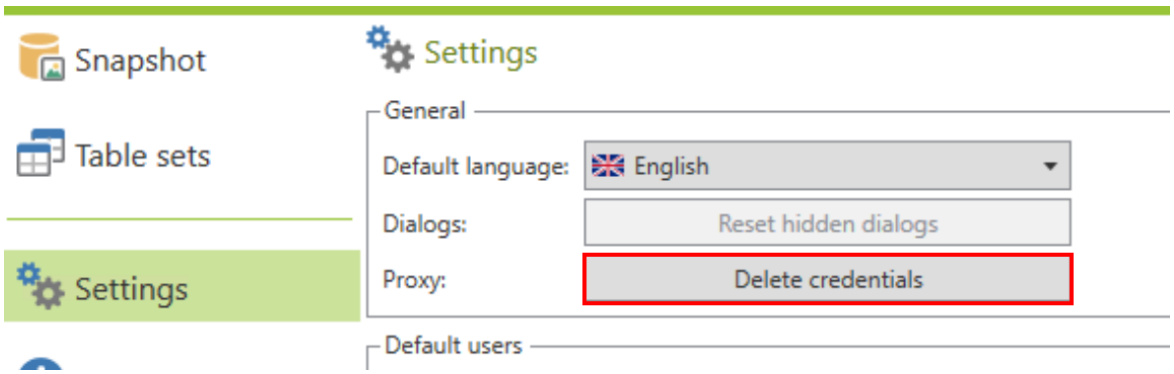



**Figure 377 - Delete login data**

The button is inactive if no data is stored in the registry.

### Update check error message

If an error occurs during the update check (e.g. because a proxy requires a login or the server cannot be reached from the internal network), the error message is displayed by an icon.

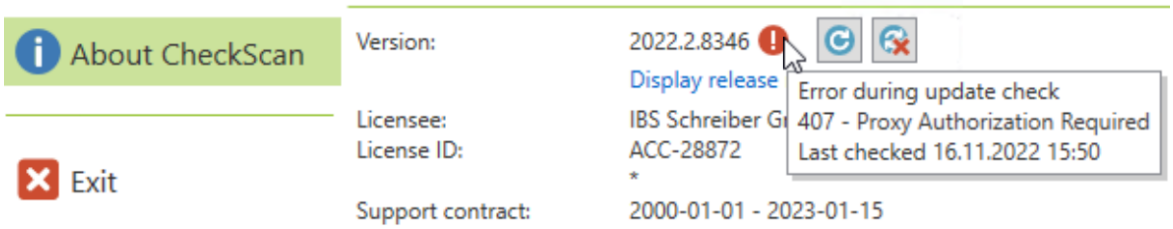



**Figure 378 - Update check error**

# Chapter IX - Property, copyright and trademarks

# IX Property, copyright and trademarks