



# iSecurity Authority Inspector

User Guide  
Version 1.1

[www.razlee.com](http://www.razlee.com)

# Contents

---

<b>About this Manual</b> .....	<b>4</b>
<b>Chapter 1 Foreword</b> .....	<b>8</b>
<b>Chapter 2 Introduction to Authority Collection</b> .....	<b>9</b>
Authority Collection Interfaces .....	12
Start Authority Collection .....	13
Authority Collection Repository Damage .....	16
Save and Restore Considerations .....	17
Authority Collection Repository .....	18
Authority Collection Active Indicator .....	19
Special Considerations .....	20
End Authority Collection .....	23
Delete Authority Collection Repository .....	24
Display Authority Collection Data .....	25
Example Queries .....	26
Analyze Authority Collection Data .....	27
AUTHORITY_COLLECTION View .....	28
Authority Field Values .....	44
Detailed Authority Field Values .....	45
<b>Chapter 3 Introduction to iSecurity Visualizer</b> .....	<b>46</b>
The iSecurity Visualizer .....	47
The Visualizer Graphical User Interface (GUI) .....	49
The Dimensions' Tabs .....	50
Tabular Results Presentation Pane .....	51
Graphical Results Presentation Pane .....	53
Graphical Analysis Toolbar .....	54
Analysis Toolbar .....	56
Status Bar .....	59
Filter Definition Pane and Selection Tabs .....	60
Filters Toolbar .....	61

---

General Issues .....	62
Initial Filter .....	63
Working with the Visualizer .....	65
Setting up Filters .....	66
Generating Reports .....	69
<b>Chapter 4 Introduction to the iSecurity Authority Inspector .....</b>	<b>70</b>
Foreword .....	71
The Demo Mode .....	73
Single Session Operation .....	75
Databases for Analysis .....	76
Installing the Authority Inspector .....	77
Uninstalling the Authority Inspector .....	83
Graphical User Interface (GUI) .....	85
The Launching Screen .....	86
Connect to System Dialog Box .....	87
Running Authority Inspector in SSL Mode .....	88
Providing Trust Store Data from Command Line .....	90
The Fields' Tabs .....	91
The Data Pane .....	92
The Analysis Toolbar .....	93
The Status Bar .....	98
Mapping of Field's Content .....	99
<b>Chapter 5 Configuring the Authority Inspector .....</b>	<b>100</b>
First-Time Launching of Authority Inspector .....	101
Configuring the Authority Inspector .....	102
The Main Menu .....	103
The Main Menu – File Sub-Menu .....	104
The Main Menu – Help Sub-Menu .....	108
<b>Chapter 6 Using the Authority Inspector .....</b>	<b>110</b>
Setting up the Filters .....	111

# About this Manual

---

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: <http://www.adobe.com/>. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the-box" security. To learn more about the iSecurity Suite, visit our website at <http://www.razlee.com/>.

## Intended Audience

The Authority Inspector User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

**NOTE:** Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

## Native IBM i (OS/400) User Interface

Authority Inspector is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

## Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on the previous page.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter, Shift-Tab**.

Emphasis is written in **Bold**.

A sequence of operations entered via the keyboard is marked as

***STRAOD > 81 > 32***

meaning: Syslog definitions activated by typing ***STRAOD*** and selecting option: **81** then option: **32**.

## Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. To select a menu option, simply type the option number and press **Enter**. The command line is

available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

## Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1: Help** Display context-sensitive help
- **F3: Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4: Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6: Add New** Create a new record or data item
- **F8: Print** Print the current report or data item
- **F9: Retrieve** Retrieve the previously-entered command
- **F12: Cancel** Return to the previous screen or menu without updating

## Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all

applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

2020 © Copyright Raz-Lee Security Inc. All rights reserved.

## Contacts

Raz-Lee Security Inc. [www.razlee.com](http://www.razlee.com)

Marketing: [marketing@razlee.com](mailto:marketing@razlee.com) 1-888-RAZLEE-4 (1-888-7295334)

Support: [support@razlee.com](mailto:support@razlee.com) 1-888-RAZLEE-2 (1-888-7295332)

# Chapter 1 Foreword

---

Raz-Lee's iSecurity Authority Inspector software application product is a component of the Raz-Lee iSecurity product line, based on the Visualizer Business Intelligence software application. Visualizer is an advanced statistical analysis tool utilizing Business Intelligence (BI) techniques to graphically analyze security related activities. Authority Inspector graphically displays and helps to analyze IBM i Security Authority Collection data, as demanded by current laws and regulations such as SOX, PCI, HIPAA, GDPR. Comprehensive details of the Visualizer application are provided in Raz-Lee's "**Visualizer Business Intelligence User Guide**" document, parts of which are quoted herein for reference.

Authority Collection is a feature provided by IBM as part of its IBM i 7.3 Operating System (OS).

It is a well-known fact among IBM i (AS/400) system administrators and security personnel that excessive user authorities are potentially a serious security hazard which needs to be avoided.

In AS/400 OS revision 7.3 IBM introduced Authority Collection which tracks authority levels allocated to users and reports, for each access, the lowest level of user authority required in order to successfully access the object.

The purpose of Authority Inspector is to turn Authority Collection raw data into information which the company can use to “fine-tune” user authorities, allocating only the level of user authorities which are required by the user in order to successfully carry out their responsibilities.



# Chapter 2 Introduction to Authority Collection

---

**NOTE:** This chapter is a part of the IBM's **Security Reference document** (Product number SC41-5302-13, covering Ver. 7.3), quoted herein for the users' convenience. All rights reserved to IBM.

Authority Collection is a capability that is provided as part of the base operating system. At a high level, Authority Collection captures data that is associated with the run-time authority checking that is built into the IBM i system. This data is logged to a repository provided by the system and interfaces are available to display and analyze the data. The intent of this support is to assist the security administrator and application provider in securing the objects in an application with the lowest level of authority that is required to allow the application to run successfully. By using the Authority Collection capability to remove or avoid excess authority, the overall security of the objects that are used by an application is improved.

Applications available for the IBM i server often have excessive authority that is granted to the objects within the application. Analysis of applications proves that this excessive authority setting is true today even with the current laws and regulations that require sensitive data to be adequately secured. Traditionally, the public authority (**\*PUBLIC**) of objects within an application is set to an authority value that exceeds the authority that is required to run the application. For example, the public authority on a DB2 table object (**\*FILE**) can be set to **\*CHANGE** authority even though the application requires **\*USE** authority to the data. This excessive authority setting opens a security exposure in the system as the data in this particular table object can be changed, outside of the application, by users of the system.

Further analysis of the application security settings shows where the authority setting is even greater than **\*CHANGE** authority. For some applications, the authority setting of **\*ALL** is used which allows users of the system to change the object and data and even delete the entire object from the system. The Authority Collection support is designed to provide the security administrator and application provider a tool to help lock down the security of the application objects.

Interfaces are provided to allow a security administrator to collect and analyze data that is associated with the authority checking support of IBM i. These interfaces support the ability to start Authority Collection for a specific user of the system. When this user runs a job on the system (interactive, batch, communication, and so on) and accesses objects within the application, Authority Collection data is gathered and written to the Authority Collection repository for the user. The data that is collected during the application's run-time authority checks is significant in both volume and detail. For this reason, you must consider the performance impact that Authority Collection has on the run-time performance of an application. While the Authority Collection can be run on a production partition, the recommendation initially is to run the Authority Collection on a test partition where the application's run-time performance requirements are not the same as the production environment. In addition, changes made to the authority settings of the objects based on the Authority Collection's data need to be fully tested before the authority changes are made in the production environment.

Authority checking support is built into the IBM i Operating System (OS) and Licensed Internal Code (LIC). Each authority check that is requested by the OS and LIC is logged to the Authority Collection data repository for the user. Access to any IBM i object (**\*FILE**, **\*PGM**, **\*CMD**, and so on) requires the authority check to succeed before access to the object and data is allowed. For the authority check to succeed, the user, the user's groups, public authority, and program adopted authority settings are considered when the system checks for authority. Each object type can have different internal implementations and thus have different authority checking requirements. This is an important detail in relation to Authority Collection. For a single IBM i OS interface (CL Command, API, Service) numerous authority checks can occur against the object(s). Consider a simple example of calling a CL

program that runs a simple command such as *DSPJOB* or *CHGJOB*. The system needs to find the library that contains the object, find the object within the library, lock the job description to prevent deletion while the interface is running, access the object itself to read (or change) the object and then display or change the data associated with the interface. Each of these steps, including locking the object, might perform an authority check against the object to make sure that the user is authorized to use the interface and target object. In fact, it is common that multiple authority checks are made by the OS and LIC for an object within a single CL command or API interface. The reason for this is that the authority checking logic built into the OS and LIC is run for internal interfaces that are used by the OS to access the object as well as the authority checks built into the interface itself.

An entry is logged in the Authority Collection repository for each unique authority check against the objects involved. This is important to understand as the authority that is required to the object must be derived from the cumulative "required authority" value from all of the Authority Collection entries that are logged for the object. For more information, see: Analyze Authority Collection Data.

## Authority Collection Interfaces

---

There are several interfaces available for the Authority Collection support.

- Start Authority Collection (*STRAUTCOL*) command
- End Authority Collection (*ENDAUTCOL*) command
- Delete Authority Collection (*DLTAUTCOL*) command
- Display User Profile (*DSPUSRPRF*) command, **\*BASIC** display, printed output, and outfile (*QADSPUPB*) will have the Authority Collection active indicator and Authority Collection repository exists indicator available.
- Display User Profile (*DSPUSRPRF*) command, **\*BASIC** display and printed output will have the *STRAUTCOL* parameters from the most recent use of *STRAUTCOL*. These values will only be shown in an Authority Collection repository currently exists for the user.
- Dump User Profile (*DMPUSRPRF*) command has the Authority Collection active indicator.
- Retrieve User Profile (*RTVUSRPRF*) command has the Authority Collection active indicator and Authority Collection repository exists indicator.
- Retrieve User Information (*QSYRUSRI*) API has the Authority Collection active indicator, Authority Collection repository exists indicator, and the Start Authority Collection (*STRAUTCOL*) command parameters.
- IBM Navigator for i, Users and Groups function, contains support for Authority Collection.
- **QSYS2.AUTHORITY\_COLLECTION** view can be used to display and analyze the Authority Collection data.
- **QSYS2.USER\_INFO** view can be used to determine which users have active Authority Collections and which users have Authority Collection repositories.

## Start Authority Collection

---

Authority Collection is based on a user. This means that the Authority Collection is only active for the "current user profile" of the job (the thread effective user profile). Authority Collection can be active for multiple users at the same time and an Authority Collection repository exists for each user. By default, the data that is collected is object level authority data for the user. Object level authority data is defined as private authorities for a user to an object (including authorities from an authorization list), group profile authority information, public authority, and program adopted authority. The intent of this support is to allow the customer to better secure their data objects with object level authority settings.

Starting Authority Collection for a group user profile can be done but the Authority Collection for this user takes effect only when the user profile (the group profile in this case) is the "current user profile" of the job (essentially, from an authority checking standpoint, the user profile is not a group profile in this situation). For example, if **USR1** has a group profile of **GRP2**, and Authority Collection is started for **GRP2**, no authority data is logged when user **USR1** is the current user of the job and **GRP2** is in the group profile list. Authority Collection for user profile **GRP2** occurs if **GRP2** is the current user of the job. In addition, starting Authority Collection for a user profile that owns a program or service program that adopts owner authority does not have authority data logged (unless this user profile is the current user of the job). For example, user profile **OWN1** owns a program that is called **PGM1** and this program adopts owner authority (**OWN1** is the program owner). If **STRAUTCOL** is run for user profile **OWN1**, and **PGM1** is called by user **USR1**, no authority data is logged under the **OWN1** Authority Collection repository. If **USR1** is specified on **STRAUTCOL**, the Authority Collection data would be logged for program **PGM1**, including the information that **PGM1** adopts the owner's authority. For group profile and adopted authority situations, significant Authority Collection information is logged to the Authority Collection repository of the current user when either the group or adopting program owner is used to satisfy an authority check.

The Start Authority Collection (**STRAUTCOL**) command is used to start the Authority Collection for a specified user profile. The command provides options to collect information for objects in libraries, document library

objects (**\*DOC** and **\*FLR** object types), and objects in the "root" (/), **QOpenSys**, and user-defined file systems.

For objects in libraries, you can select which libraries, objects (including generic names), and object types to include in the Authority Collection for the specified user. In addition, an Omit Library (**OMITLIB**) parameter is available to omit certain libraries and corresponding objects from the Authority Collection.

For document library objects and file system objects, **STRAUTCOL** provides an option to include information only about specific object types. While the collection itself cannot be restricted to particular objects, folders, or directories, the interfaces provided for analyzing a collection are fully capable of selecting and reporting data only for specific objects of interest.

The Detail (**DETAIL**) parameter on the **STRAUTCOL** command specifies the details that are used to determine whether an authority check is for a unique instance. One unique instance is collected for each check. The **\*OBJINF** value indicates that the authority checking information is collected for each unique instance of the object level information that is associated with the authority check. Specifying this value results in the collection of object level unique authority checks regardless of the job that accesses the object and regardless of the unique code paths within the job. The **\*OBJJOB** value indicates that the authority checking information is collected for each unique instance of the object level information that is associated with the authority check and each unique instance of the job information that is associated with the authority check. Specifying this value results in the collection of object and job level unique authority checks plus each unique code path within the job is collected. For examples, see the Start Authority Collection (**STRAUTCOL**) command.

Authority Collection for a specified user can be started by using the **STRAUTCOL** command and ended by using the **ENDAUTCOL** command.

Authority Collection can be restarted for a user after it has been ended by using the **STRAUTCOL** command. This provides the capability to collect additional authority data when the Authority Collection is restarted.

To collect authority information for the users that an application runs under:

1. Start Authority Collection for the user the application runs under. If the application runs under different users, then start Authority Collection for each user.
2. Run the application.
3. End Authority Collection for each user.
4. Analyze the authority data that is collected for each user.

## Authority Collection Repository Damage

---

Damage can occur to the Authority Collection repository for a user.

The damage can frequently occur in the case of an abnormal IPL of the partition where Authority Collection is active for one or more users. For performance reasons, Authority Collection data is not immediately written out to disk when it is collected. Forcing the data to disk would result in unacceptable performance for the Authority Collection due to the volume and frequency of data that is written to the repository. If an abnormal IPL occurs when Authority Collection is active, the recovery is to delete the authority collection repository, if damaged, for the user(s) using the Delete Authority Collection (*DLTAUTCOL*) command and then start the authority collection again.

To determine which Authority Collection repositories need to be deleted, use the following SQL query:

```
SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
    QSYS2.USER_INFO WHERE
    AUTHORITY_COLLECTION_REPOSITORY_EXISTS='YES';
```

Before an Authority Collection repository can be deleted using the *DLTAUTCOL* command, Authority Collection for the user must first be ended using the End Authority Collection (*ENDAUTCOL*) command. The **AUTHORIZATION\_NAME** values returned by the query should be used on the *ENDAUTCOL* and *DLTAUTCOL* commands.

Unfortunately, this damage results in the loss of the previously collected authority data. Note that a DB2 table object can be created at any time from the active authority collection data. This creates a "snapshot" of the data. If Authority Collection is run over an extended period, a table object can be periodically created and updated to prevent data loss if an abnormal IPL occurs.



## Save and Restore Considerations

---

The Authority Collection data repository for a user is not saved or restored.  
The Authority Collection active indicator in the user profile is saved and restored.

## Authority Collection Repository

There is no support on the Save Security Data (*SAVSECDTA*) command, or any other save interface, to save the Authority Collection data for a user. To save the Authority Collection data, it must first be written to a DB2 table (*\*FILE* object) by querying the *QSYS2.AUTHORITY\_COLLECTION* view. See Display Authority Collection Data for an example of writing the Authority Collection data to a table. The DB2 table object can then be saved and restored if necessary.

## Authority Collection Active Indicator

The Authority Collection active indicator in the user profile is saved for each profile when using the *SAVSECDTA* command.

When a profile is restored using the Restore User Profile (*RSTUSRPRF*) command the Authority Collection active indicator is restored as follows:

- If the profile on the media has Authority Collection active then a check is made to see if the Authority Collection repository for the user exists on the system. If it does, then the restored user profile will have Authority Collection active. If it does not, then the restored user profile will have Authority Collection turned off with the End Authority Collection (*ENDAUTCOL*) command.
- If the profile on the media does not have Authority Collection active then the restored user profile will not have Authority Collection active.

## Special Considerations

---

Special considerations for Authority Collection:

1. The Authority Collection support does NOT collect data that is related to interfaces that check special authority. Authority Collection data that is related to **\*ALLOBJ** special authority is collected as it affects object level security. Other special authority checks, authorities such as **\*JOBCTL** or **\*SAVSYS**, do not generate Authority Collection entries. Special authority settings for a specific user profile are easy to check by using the existing security interfaces such as the Display User Profile (*DSPUSRPRF*) command and related APIs or by querying the **QSYS2.USER\_INFO** view.
2. Function usage settings (also called application administration) are not collected for the same reason as special authority settings. Function usage settings for a specific user profile are easy to check and are managed by using the Work with Function Usage (*WRKFCNUSG*) command or by querying the **QSYS2.FUNCTION\_USAGE** view.
3. The system automatically excludes certain system libraries and their objects, such as **QRCL**, **QSPL**, **QTEMP**, **QPTFOBJ1**, or **QPTFOBJ2** (and the corresponding IASP version of the system libraries), from the Authority Collection data. Also excluded are authority checks against objects that are not in a library, folder, or directory.
4. The system automatically excludes system programs and service programs from the Authority Collection data. Programs or service programs that are **\*SYSTEM** domain or have a program state of **\*SYSTEM** or **\*INHERIT** are excluded from the Authority Collection. These attributes can be displayed by using the Display Program (*DSPPGM*) and Display Service Program (*DSPSRVPGM*) commands.

5. The system automatically excludes Authority Collection data when the IBM i operating system accesses an object and authority is available because of program adopted authority from the operating system. The operating system uses program adopted authority to manage and secure objects and control blocks that it uses. In addition, the operating system uses program adopted authority for situations where it requires access to an object for a specific reason and the current user of the job is not authorized.
6. The system automatically excludes Authority Collection data for document library objects and file system objects that have been deleted.
7. The open file (**\*FILE** objects) support for Authority Collection is for full opens only (no shared or pseudo open is logged).  
The initial Authority Collection occurs at file open but the data is not written to the Authority Collection repository until a hard close on the file is done.

Writing the Authority Collection data to the repository for the file open/close case must be done at close time to accurately log the authority that is required (the open might be done for read/add/update/delete but the application might only read the data) for the application.

8. Authority Collection of column permissions for a DB2 table is not supported.
9. If the **STRAUTCOL** command is used to start the Authority Collection for a user profile and the partition is **IPLed**, the Authority Collection continues when a job (post IPL) running under the specified user profile starts.
10. IBM i supports a capability that is called profile swap. A profile swap can occur within an active job to swap the current user of a thread from one user to another. When this profile swap occurs, the Authority Collection of the previous user, for this thread, is no longer active because the current user changed.

If the newly swapped user has Authority Collection active, any authority checks made are now logged under this user's Authority Collection repository.

11. If a user profile with an active Authority Collection is deleted, the Authority Collection is automatically ended before the user profile is deleted.
12. To collect authority information for object types that are only allowed in **QSYS** (for example, **\*LIB**), specify parameter **LIBINF(\*ALL)** on the **STRAUTCOL** command. When Authority Collection includes object type **\*LIB**, library objects that start with **QSYS\*** are automatically excluded from the Authority Collection data.
13. When Authority Collection is started for a user that has an existing authority collection data repository, new authority data is added to the existing information unless parameter **DLTCOL(\*YES)** is specified. New Authority Collection data can only be added to the existing information if the value specified on the **DETAIL** parameter matches the value that was specified on the **DETAIL** parameter when the existing authority information was collected.

## End Authority Collection

---

Authority Collection can be ended for a specified user.

The End Authority Collection (*ENDAUTCOL*) command stops the Authority Collection for the specified user. The *ENDAUTCOL* command must be run after all jobs that are running under the specified user have ended to ensure that all of the information for this user is collected. For DB2 objects of type **\*FILE**, collecting authority information occurs during file open, subsequent file I/O, and the file close. A full close of the **\*FILE** must be done for complete authority information to be collected for the object.

Authority Collection for a specified user can be started by using the *STRAUTCOL* command and ended by using the *ENDAUTCOL* command. Authority Collection can be restarted for a user after it has been ended by using the *STRAUTCOL* command. This provides the capability to collect additional authority data when the Authority Collection is restarted.

Ending Authority Collection for the user does not delete the Authority Collection repository. The data remains in the repository until the repository is deleted.

## Delete Authority Collection Repository

---

The Authority Collection repository for a user can be deleted.

The Delete Authority Collection (*DLTAUTCOL*) command deletes the Authority Collection data repository for the specified user. Deleting the Authority Collection data repository deletes all Authority Collection information for the specified user. The Authority Collection data repository can also be deleted when the Start Authority Collection (*STRAUTCOL*) command is run using the *DLTCOL* parameter. To save the Authority Collection data before using *DLTAUTCOL*, it must first be written to a DB2 table (*\*FILE* object) by using the provided view support. See Display Authority Collection Data for an example of writing the Authority Collection data to a table.



## Display Authority Collection Data

---

Authority Collection captures a significant amount of information that is associated with the authority checking of an object. The SQL view **QSYS2.AUTHORITY\_COLLECTION** is used to display and analyze this information.

IBM Navigator for i shows the Authority Collection information for a specific user but not in a form that can be queried. IBM Navigator for i has interfaces for Authority Collection within the Users and Groups function.

- There are nodes in the console navigation area for starting, ending, displaying, and deleting Authority Collection for a user.
- There are tasks available for a user within the User list to start, end, display, and delete Authority Collection.
- An Authority Collection tab on the Capabilities page of the User properties panel shows the current Authority Collection status for the user.
- There is a table view of the items included in the Authority Collection. This can be viewed in a web table, or in a client viewer if IBM i Access Client Solutions (ACS) is installed on the PC. The web table will also support Properties and Permissions actions for each object that appears in the list.

The Run SQL Scripts function in Navigator for i can be used to query the **AUTHORITY\_COLLECTION** View. Some SQL query examples that can be run against the view are shown below.

## Example Queries

View Authority Collection data for **USER1**.

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION
    WHERE USER_NAME = 'USER1'
```

View Authority Collection data for **USER1** for object **PAYROLL** in library **PAYLIB**.

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION
    WHERE USER_NAME = 'USER1' AND
    SYSTEM_OBJECT_NAME = 'PAYROLL' AND SYSTEM_OBJECT_SCHEMA = 'PAYLIB'
```

View Authority Collection data for **USER1**, object **PAYROLL** in **PAYLIB**, and object type **\*FILE**.

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION
    WHERE USER_NAME = 'USER1' AND
    SYSTEM_OBJECT_NAME = 'PAYROLL' AND SYSTEM_OBJECT_SCHEMA = 'PAYLIB'
    AND SYSTEM_OBJECT_TYPE = '*FILE'
```

Save the Authority Collection data for **USER1** to **DB2** table **MYLIB.MYFILE**.

Writing the Authority Collection data to a **DB2** table allows the data to be saved and restored to another partition. The **DB2 ~** table can then be analyzed by querying the resulting **DB2** table.

```
CREATE TABLE MYLIB.MYFILE AS
    (SELECT * FROM AUTHORITY_COLLECTION WHERE USER_NAME = 'USER1') WITH
    DATA
SELECT * FROM MYLIB.MYFILE
```

## Analyze Authority Collection Data

---

The Authority Collection data can be analyzed to help you secure the objects in an application.

The **detailed required authority** value returned in the **DETAILED\_REQUIRED\_AUTHORITY** field by the **QSYS2.AUTHORITY\_COLLECTION** view is a key piece of information available to help the security administrator or application owner better secure the object. The detailed required authority value represents the authority the system requires in order to pass the authority check against the object. By analyzing the detailed required authority value from **every** Authority Collection entry for a given object you can determine the minimum level of authority that can be granted to an object and still allow the application to run successfully.

To generate the Authority Collection entries for an object you must run the application to completion taking into account all code paths within the application. For example, if the application has special processing for end of quarter or year end, you must consider these code paths as well as the normal run-time processing within the application. Once the Authority Collection entries have been generated, the detailed required authority values from the Authority Collection will determine what authority the user needs to run the application successfully. If the detailed required authority value from all Authority Collection entries is less than the users current authority, the excess authority can be revoked for this user (or group or **\*PUBLIC**) in order to set the authority to the lowest possible value and better secure the object.

Two Authority Collection values returned by the **QSYS2.AUTHORITY\_COLLECTION** view, **DETAILED\_CURRENT\_AUTHORITY** and **DETAILED\_CURRENT\_ADOPTED\_AUTHORITY**, will provide the authority values available in the job at the time of the authority check. The authority available in the job comes from the user's authority, the authority from any group user profiles, public authority and adopted authority from the owner of currently running programs or service programs in the job. The **AUTHORITY\_SOURCE** and **ADOPTED\_AUTHORITY\_SOURCE** values returned by the view indicate the source of authority used for the authority check data that is captured and logged in each Authority Collection entry.

## AUTHORITY\_COLLECTION View

---

The `AUTHORITY_COLLECTION` view contains information about the authority check for an object.

The following table describes the columns in the view. The schema is `QSYS2`.

Column Name	System Column Name	Data Type	Description
AUTHORIZATION_NAME	USER_NAME	VARCHAR(10) Nullable	The name of the user profile for which authority information was collected.
CHECK_TIMESTAMP	CHKTIME	TIMESTAMP Nullable	The date and time the authority check was made.
SYSTEM_OBJECT_NAME	SYS_ONAME	CHAR(10) Nullable	The name of the object whose authority was checked. This field contains information for objects in libraries and document library objects ( <b>*DOC</b> and <b>*FLR</b> object types). Document library objects in this field will be in <b>*SYSOBJNAM</b> format. File system objects and document library objects use the <b>PATH_NAME</b> field.
SYSTEM_OBJECT_SCHEMA	SYS_DNAME	CHAR(10) Nullable	The name of the library that contains the object.
SYSTEM_OBJECT_TYPE	SYS_OTYPE	CHAR(8) Nullable	The object type of the object.
ASP_NAME	ASP_NAME	CHAR(10) Nullable	The name of the auxiliary storage pool to which storage for the object is allocated.
ASP_NUMBER	ASP_NUMBER	DECIMAL(5,0) Nullable	The number of the auxiliary storage pool to which storage for the object is allocated. A value of 0 indicates <b>*SYSBAS</b>
OBJECT_NAME	ONAME	VARCHAR(128) Nullable	The SQL name of the object. Objects supported by SQL may have the same name a longer name than the IBM i name ( <b>SYSTEM_OBJECT_NAME</b> ).
OBJECT_SCHEMA	OSHEMA	VARCHAR(128) Nullable	The SQL name of the schema (library). Schema in SQL may have the same name as the IBM i name or may have a different longer name than the IBM i name ( <b>SYSTEM_OBJECT_SCHEMA</b> ).
OBJECT_TYPE	OTYPE	VARCHAR(9)	The SQL object type. The

Column Name	System Column Name	Data Type	Description
		Nullable	<p>following values can be returned.</p> <ul style="list-style-type: none"> <li>• <b>ALIAS</b> – The object is an SQL alias.</li> <li>• <b>FUNCTION</b> – The object is an SQL function.</li> <li>• <b>INDEX</b> – The object is an SQL index.</li> <li>• <b>PACKAGE</b> – The object is an SQL package.</li> <li>• <b>PROCEDURE</b> – The object is an SQL procedure.</li> <li>• <b>ROUTINE</b> – The object is used in SQL by one or more external functions and/or external procedures.</li> <li>• <b>SEQUENCE</b> – The object is an SQL sequence.</li> <li>• <b>TABLE</b> – The object is an SQL table.</li> <li>• <b>TRIGGER</b> – The object is an SQL trigger.</li> <li>• <b>TYPE</b> – The object is an SQL type.</li> <li>• <b>VARIABLE</b> – The object is an SQL global variable.</li> <li>• <b>VIEW</b> – The object is an SQL view.</li> <li>• <b>XSR</b> – The object is an XML schema repository object.</li> </ul>
AUTHORIZATION _ LIST	AUTL	CHAR(10)  Nullable	<p>The name of the authorization list used to secure the object.</p> <p>This field contains data only if the object is secured by an authorization list</p>
AUTHORITY_ CHECK_ SUCCESSFUL	CHKSUCCESS	CHAR(1)  Nullable	<p>The result of the authority check. This field is set to '1' if the authority check was successful and '0' if the authorities check</p>

Column Name	System Column Name	Data Type	Description
			was not successful.
CHECK_ANY_AUTHORITY	CHKANYAUTH	CHAR(1)  Nullable	<p>Indicates whether the authority check that is performed by the system is for "ANY" or the authorities that are listed in the <b>DETAILED_REQUIRED_AUTHORITY</b> field.</p> <p>This field is set to '1' if "ANY" of the authorities were checked and '0' if specific authorities were checked.</p> <p>Certain authority checks allow the function to complete if the user associated with the currently running job has one or more of the authorities that are listed in the <b>DETAILED_REQUIRED_AUTHORITY</b> field.</p> <p>A common function that performs the "ANY" authority check is the system lock instruction that is used by many system commands, APIs, and services.</p>
CACHED_AUTHORITY	CACHEAUTH	CHAR(1)  Nullable	<p>The operating system (OS) and Licensed Internal Code (LIC) have the capability to cache the authority the user currently has to an object, and use this authority for future authority checks.</p> <p>This field is set to '1' if authority was cached and '0' if authority was not cached.</p> <p>For performance reasons, the Authority Collection code will log, to the Authority Collection repository, the first authority check where cached authority is initially stored.</p>

Column Name	System Column Name	Data Type	Description
			<p>Future authority checks, that use the cached authority, are not logged to the Authority Collection repository. However, any future authority check that required more authority than was initially cached results in the logging of an Authority Collection entry for the authority check.</p> <p>In addition, the Authority Collection entries that have this field set to '1' might not always provide an accurate view of the required authority information. The reason for this is that the system code can cache the maximum authority the current user of the job has to the object but require only a subset of this authority to pass a future authority check.</p> <p>This is a rare case within the <b>OS</b> and <b>LIC</b> but might occasionally be done.</p>
REQUIRED_ AUTHORITY	REQAUTH	VARCHAR(7)  Nullable	<p>The authority that is required by the system to access the object.</p> <p>If the <b>DETAILED_REQUIRED_AUTHORITY</b> field does not map to a system-defined object authority level, this field will be blank.</p> <p>See "Authority Field Values" on page 44.</p>
DETAILED_ REQUIRED_ AUTHORITY	DTLREQAUTH	VARCHAR(90)  Nullable	<p>The detailed individual authority values that are required by the system to access the object.</p> <p>This is an important piece of information in the Authority Collection data.</p> <p>The detailed required authority is what is used to determine what</p>



Column Name	System Column Name	Data Type	Description
			<p>authority can be set on the object so that it passes the authority check.</p> <p>Analyzing all of the Authority Collection entries for an object indicate what authority value can be set on the object to allow the application to run successfully from an authority standpoint.</p> <p>See "Detailed Authority Field Values" on page 45.</p>
<b>CURRENT_AUTHORITY</b>	<b>CURAUTH</b>	VARCHAR(8)  Nullable	<p>The authority that the user currently has to the object.</p> <p>The <b>AUTHORITY_SOURCE</b> field must also be evaluated to determine where the users' authority to the object was found.</p> <p>If the <b>DETAILED_CURRENT_AUTHORITY</b> field does not map to a system-defined object authority level, this field will be blank.</p> <p>See "Detailed Authority Field Values" on page 45.</p>
<b>DETAILED_CURRENT_AUTHORITY</b>	<b>DTLCURAUTH</b>	VARCHAR(99)  Nullable	<p>The detailed authority values that the user currently has to the object.</p> <p>The <b>AUTHORITY_SOURCE</b> field must also be evaluated to determine where the users' authority to the object was found.</p> <p>See "Detailed Authority Field Values" on page 45.</p>
<b>AUTHORITY_SOURCE</b>	<b>AUTHSRE</b>	VARCHAR(50)  Nullable	<p>Where the system found the authority that either satisfied the authority check or caused the authority check to end unsuccessfully.</p>

Column Name	System Column Name	Data Type	Description
			<ul style="list-style-type: none"> <li>• <b>USER *ALLOBJ</b> – All object special authority from the user</li> <li>• <b>USER OWNERSHIP</b> – User ownership</li> <li>• <b>USER PRIVATE</b> – User private authority</li> <li>• <b>AUTHORIZATION LIST OWNERSHIP</b> – Authorization list ownership</li> <li>• <b>AUTHORIZATION LIST PRIVATE</b> – Authorization list private authority</li> <li>• <b>GROUP *ALLOBJ</b> – Group profile all object special authority</li> <li>• <b>GROUP OWNERSHIP</b> – Group ownership</li> <li>• <b>GROUP PRIVATE</b> – Group private authority</li> <li>• <b>PRIMARY GROUP</b> – Primary group authority</li> <li>• <b>AUTHORIZATION LIST GROUP OWNERSHIP</b> – Authorization list group ownership</li> <li>• <b>AUTHORIZATION LIST PRIMARY GROUP</b> – Authorization list primary group authority</li> <li>• <b>AUTHORIZATION LIST GROUP PRIVATE</b> – Authorization list group private authority</li> <li>• <b>AUTHORIZATION LIST PUBLIC</b> – Authorization list public authority</li> <li>• <b>PUBLIC</b> – Public authority</li> </ul>

-

Column Name	System Column Name	Data Type	Description
			<ul style="list-style-type: none"> <li>Also see the <b><i>ADOPTED_AUTHORITY_SOURCEG</i></b> field</li> </ul>
GROUP_NAME	GROUP_NAME	CHAR(10)  Nullable	<p>The name of the group profile whose authority was used to satisfy the authority check.</p> <p>If multiple group profiles contribute to the accumulated current authority for the object, this field contains the last group to contribute and the <b>MULTIPLE_GROUPS_USED</b> field is set to '1'. Group profiles are checked for authority based on the order in the group profile and supplemental group profile list in the user profile.</p>
MULTIPLE_GROUPS_USED	MLTGRPUSED	CHAR(1)  Nullable	<p>Indicates whether multiple group profiles contributed to the <b><i>DETAILED_CURRENT_AUTHORITY</i></b> for the object.</p> <p>This field is set to '1' if multiple group profiles contributed and '0' if no group profiles or only one group profile's authority is used.</p>
ADOPT_AUTHORITY_USED	ADOPTUSED	CHAR(1)  Nullable	<p>Indicates whether adopted authority is used to satisfy the authority check. This field is set to '1' if the authority of the adopting program owner is used to satisfy the authority check.</p> <p>This field is set to '0' if adopted authority was not used to satisfy the authority check.</p> <p>In addition, when this field is set to '0', the <b>ADOPTING_PROGRAM_NAME</b> field can contain the name of a program that is on the program invocation stack of the thread.</p>

Column Name	System Column Name	Data Type	Description
			<p>If a program is listed, this program adopts the owners' authority and would satisfy the authority check if authority was not available from another authority source in the thread. That is, excessive authority could be removed, and adopted authority used. If no program name is listed in the <b>ADOPTING_PROGRAM_NAME</b> field, then this indicates no program in the invocation stack would satisfy the authority check for the object.</p>
<b>MULTIPLE_ADOPTING_PROGRAMS_USED</b>	<b>MLTADOPTPG</b>	CHAR(1)  Nullable	<p>Indicates whether the owners of multiple programs that adopt contribute authority to the combined <b>DETAILED_CURRENT_ADOPTED_AUTHORITY</b> field.</p> <p>This field is set to '1' if multiple programs that adopt contributed and '0' if no programs that adopt or only one program that adopts is used.</p>
<b>ADOPTING_PROGRAM_NAME</b>	<b>ADOPTPGM</b>	CHAR(10)  Nullable	<p>The name of the program that adopts the owners' authority. If multiple adopting programs contribute to the accumulated <b>DETAILED_CURRENT_ADOPTED_AUTHORITY</b> for the object, the last program to contribute is listed and the <b>MULTIPLE_ADOPTING_PROGRAMS_USED</b> field is set to '1'.</p> <p>Adopting programs are checked for authority in order from the most recent invocation to the oldest invocation on the program invocation stack.</p>

Column Name	System Column Name	Data Type	Description
ADOPTING_ PROGRAM_ SCHEMA	ADOPTLIB	CHAR(10)  Nullable	The name of the library that contains the adopting program.
ADOPTING_ PROCEDURE_ NAME	ADOPTPRC	VARCHAR(256)  Nullable	The name of the adopting Integrated Language Environment (ILE) program procedure.
ADOPTING_ PROGRAM_ TYPE	ADOPTPGMT	CHAR(8)  Nullable	The object type of the adopting program.
ADOPTING_ PROGRAM_ ASP_ NAME	ADOPTPGMA	CHAR(10)  Nullable	The name of the auxiliary storage pool to which storage for the adopting program is allocated.
ADOPTING_ PROGRAM_ ASP_ NUMBER	ADOPTPGMAN	DECIMAL(5,0)  Nullable	The number of the auxiliary storage pool to which storage for the adopting program is allocated.  A value of 0 indicates <b>*SYSBAS</b> .
ADOPTING_ PROGRAM_ STATEMENT_ NUMBER	ADOPTPGMSN	DECIMAL(10,0)  Nullable	The statement number of the adopting program.
ADOPTING_ PROGRAM_ OWNER	ADOPTPGMOW	CHAR(10)  Nullable	The name of the adopting program owner.  The adopting program owners' authority is included in the authority checking algorithm of the system when the program in the <b>ADOPTING_PROGRAM_NAME</b> field is on the program invocation stack.  <b>Note:</b> The ability to block adopted authority from previous invocations exists, by using the Use Adopted Authority attribute of a program.  This attribute can be changed by using the Change Program ( <b>CHGPGM</b> ) command.  When the Use Adopted Authority

Column Name	System Column Name	Data Type	Description
			value of <b>*NO</b> is set on a program, this prevents any adopted authority from previous invocations from being included in the authority checking algorithm of the system.
CURRENT_ADOPTED_AUTHORITY	CURADPT	VARCHAR(8)  Nullable	<p>The authority value that the adopting program owner currently has to the object.</p> <p>The <b>ADOPTED_AUTHORITY_SOURCE</b> field must also be evaluated to determine where the adopting program owners' authority to the object was found. If the <b>DETAILED_CURRENT_ADOPTED_AUTHORITY</b> field does not map to a system-defined object authority level, this field will be blank.</p> <p>See "Authority Field Values" on page 44.</p>
DETAILED_CURRENT_ADOPTED_AUTHORITY	DTLCURADPT	VARCHAR(99)  Nullable	<p>The detailed authority values that the adopting program owner currently has to the object.</p> <p>The <b>ADOPTED_AUTHORITY_SOURCE</b> field must also be evaluated to determine where the adopting program owners' authority to the object was found.</p> <p>See "Detailed Authority Field Values" on page 45.</p>
ADOPTED_AUTHORITY_SOURCE	ADOPTAUTSR	VARCHAR(50)  Nullable	<p>Where the system found the adopted authority that either satisfied the authority check or caused the authority check to end unsuccessfully.</p> <ul style="list-style-type: none"> <li>• <b>ADOPTED *ALLOBJ</b> – All object special authority from the adopting program owner.</li> </ul>

Column Name	System Column Name	Data Type	Description
			<ul style="list-style-type: none"> <li>• <b>ADOPTED OWNERSHIP</b> – Adopted ownership from the adopting program owner.</li> <li>• <b>ADOPTED PRIMARY GROUP</b> – Adopted primary group authority from the adopting program owner.</li> <li>• <b>ADOPTED PRIVATE</b> – Adopted private authority from the adopting program owner.</li> <li>• <b>ADOPTED AUTHORIZATION LIST OWNERSHIP</b> – Adopted authorization list ownership from the adopting program owner.</li> <li>• <b>ADOPTED AUTHORIZATION LIST PRIMARY GROUP</b> – Adopted authorization list primary group authority from the adopting program owner.</li> <li>• <b>ADOPTED AUTHORIZATION LIST PRIVATE</b> – Adopted authorization list private authority from the adopting program owner.</li> </ul>
<b>MOST_RECENT_PROGRAM_INVOKED</b>	<b>PGMINV</b>	CHAR(10)  Nullable	The name of the most recent program on the program invocation stack when the authority check was made.
<b>MOST_RECENT_PROGRAM_SCHEMA</b>	<b>PGMLIBINV</b>	CHAR(10)  Nullable	The name of the library that contains the most recent program invoked.
<b>MOST_RECENT_</b>	<b>MODINV</b>	VARCHAR(30)	The name of the bound module

Column Name	System Column Name	Data Type	Description
MODULE		Nullable	within the most recently invoked ILE program.
MOST_RECENT_PROGRAM_PROCEDURE	PGMPRC	VARCHAR(256) Nullable	The name of the most recently invoked ILE program procedure.
MOST_RECENT_PROGRAM_TYPE	PGMTYP	CHAR(8) Nullable	The object type of the most recent program invoked.
MOST_RECENT_PROGRAM_ASP_NAME	PGMASP	CHAR(10) Nullable	The name of the auxiliary storage pool to which storage for the most recent program is allocated.
MOST_RECENT_PROGRAM_ASP_NUMBER	PGMASPN	DECIMAL(5,0) Nullable	The number of the auxiliary storage pool to which storage for the most recent program is allocated. A value of 0 indicates <b>*SYSBAS</b> .
MOST_RECENT_PROGRAM_STATEMENT_NUMBER	PGMSTMN	DECIMAL(10,0) Nullable	The statement number of the most recent program.
MOST_RECENT_USER_STATE_PROGRAM_INVOKED	USTPGM	CHAR(10) Nullable	The name of the most recent user state program on the program invocation stack when the authority check was made. A user state program is a program that is not part of the System State portion of the IBM i OS or the System State portion of an IBM product. Programs created by customers, programs created by application providers, and many products provided by IBM run in user state.
MOST_RECENT_USER_STATE_PROGRAM_SCHEMA	USTLIB	CHAR(10) Nullable	The name of the library that contains the most recent user state program invoked.
MOST_RECENT_USER_STATE_	USTMOD	VARCHAR(30)	The name of the bound module within the most recently invoked



Column Name	System Column Name	Data Type	Description
MODULE		Nullable	user state ILE program.
MOST_RECENT_USER_STATE_PROGRAM_PROCEDURE	USTPGMPRC	VARCHAR(256)  Nullable	The name of the most recently invoked user state ILE program procedure.
MOST_RECENT_USER_STATE_PROGRAM_TYPE	USTPGMTYP	CHAR(8)  Nullable	The object type of the most recent user state program invoked.
MOST_RECENT_USER_STATE_PROGRAM_ASP_NAME	USTPGMASP	CHAR(10)  Nullable	The name of the auxiliary storage pool to which storage for the most recent user state program is allocated.
MOST_RECENT_USER_STATE_PROGRAM_ASP_NUMBER	USTPGMASPN	DECIMAL(5,0)  Nullable	The number of the auxiliary storage pool to which storage for the most recent user state program is allocated. A value of 0 indicates <b>*SYSBAS</b> .
MOST_RECENT_USER_STATE_PROGRAM_STATEMENT_NUMBER	USTPGMSN	DECIMAL(10,0)  Nullable	The statement number of the most recent user state program.
JOB_NAME	JOB_NAME	CHAR(10)  Nullable	The job name of the job in which the authority check was made.
JOB_USER	JOB_USER	CHAR(10)  Nullable	The job user of the job in which the authority check was made.
JOB_NUMBER	JOBNBR	CHAR(6)  Nullable	The job number of the job in which the authority check was made.
THREAD_ID	THREAD_ID	BIGINT  Nullable	The thread ID of the currently running thread of the job in which the authority check was made.
CURRENT_USER	CURUSR	CHAR(10)  Nullable	The current user associated with the thread of the job in which the authority check was made.
OBJECT_FILE_ID	OFILEID	BINARY(16)  Nullable	The file ID of the path name.

Column Name	System Column Name	Data Type	Description
OBJECT_ASP_NAME	OASP	VARCHAR(10)  Nullable	The name of the auxiliary storage pool to which storage for the object in the path name is allocated.
OBJECT_ASP_NUMBER	OASPN	DECIMAL(5,0)  Nullable	The number of the auxiliary storage pool to which storage for the object in the path name is allocated.  A value of 0 indicates <b>*SYSBAS</b> .
PATH_NAME	PATH_NAME	DBCLOB(16M) CCSID 1200 Nullable	The path of the object whose authority was checked.  This field contains information for document library objects ( <b>*DOC</b> and <b>*FLR</b> object types), and objects in the "root" (/), <b>QOpenSys</b> , and user-defined file systems.  This field will not be filled in for objects in libraries.
PATH_REGION	PATHREGION	CHAR(2) Nullable	The country or region id for the path name.
PATH_LANGUAGE	PATHLANG	CHAR(3) Nullable	The language id for the path name.
ABSOLUTE_PATH_INDICATOR	ABSPATHIND	CHAR(1)  Nullable	Indicates whether the path name of the object is an absolute path or a relative path.  This field is set to 'Y' if the path name of the object begins with a delimiter (path name resolution starts at the "root" (/) directory).  This field is set to 'N' if the path name of the object contains a relative path name.  In addition, when this field contains 'N', the <b>RELATIVE_DIRECTORY_FILE_ID</b> field contains the File ID of the parent directory of the relative path which is used to form an absolute

Column Name	System Column Name	Data Type	Description
			path name.
RELATIVE_DIRECTORY_FILE_ID	RELDIRID	BINARY(16)  Nullable	The relative directory file's ID of the parent directory that contains the object in the <b>PATH_NAME</b> field.  This field is set when the <b>ABSOLUTE_PATH_INDICATOR</b> field is 'N'.

## Authority Field Values

The `REQUIRED_AUTHORITY` field, `CURRENT_AUTHORITY` field, and `CURRENT_ADOPTED_AUTHORITY` field can contain one of the values listed below.

- **\*ALL** – Allows all operations on the object except those that are limited to the owner or controlled by authorization list management authority. This value is made up of the following detailed authority values: **\*OBJEXIST**, **\*OBJMGT**, **\*OBJOPR**, **\*OBJALTER**, **\*OBJREF**, **\*READ**, **\*ADD**, **\*DLT**, **\*UPD**, **\*EXECUTE**.
- **\*CHANGE** – Allows all operations on the object except those that are limited to the owner or controlled by object existence authority, object alter authority, object reference authority, and object management authority. This value is made up of the following detailed authority values: **\*OBJOPR**, **\*READ**, **\*ADD**, **\*DLT**, **\*UPD**, **\*EXECUTE**.
- **\*USE** – Allows access to the object attributes and use of the object. The user cannot change the object. This value is made up of the following detailed authority values: **\*OBJOPR**, **\*READ**, **\*EXECUTE**.
- **\*EXCLUDE** – All operations on the object are prohibited.

## Detailed Authority Field Values

The `DETAILED_REQUIRED_AUTHORITY` field, `DETAILED_CURRENT_AUTHORITY` field, and `DETAILED_CURRENT_ADOPTED_AUTHORITY` field can contain one or more of the values listed below.

- **\*OBJALTER:** Object alter – provides authority to change the attributes of an object, such as adding or removing triggers and adding members for a database file.
- **\*OBJEXIST:** Object existence – provides authority to control the object's existence and ownership.
- **\*OBJMGT:** Object management – provides authority to specify security, to move or rename the object, and to add members if the object is a database file.
- **\*OBJOPR:** Object operational – provides authority to look at the object's attributes and to use the object as specified by the data authorities that the user has to the object.
- **\*OBJREF:** Object reference – provides authority to specify the object as the first level in a referential constraint.
- **\*ADD:** Add – provides authority to add entries to the object.
- **\*DLT:** Delete – provides authority to remove entries from the object.
- **\*EXECUTE:** Execute – provides authority to run a program or search a library or directory.
- **\*READ:** Read – provides authority to access the contents of the object.
- **\*UPD:** Update – provides authority to change the content of existing entries in the object.
- **\*EXCLUDE:** Exclude – all operations on the object are prohibited.
- **\*AUTLMGT:** Authorization list management – the authority required to add, change or remove users and their authority from an Authorization List object.
- **\*OWNER:** Ownership – the user owns the object and has all object and data authorities.

# Chapter 3 Introduction to iSecurity Visualizer

---

**NOTE:** A complete explanations of iSecurity Visualizer can be found in Raz-Lee's "**Visualizer Business Intelligence User Guide**" document.

## The iSecurity Visualizer

---

Raz-Lee's iSecurity Visualizer application is an advanced data analysis tool that grants IT managers the ability to dynamically, interactively, intuitively and graphically analyze and segment security-related system activity quickly and easily.

The Visualizer utilizes On Line Analytical Processing (OLAP) techniques, a widely accepted approach for swift queries in Multi-Dimensional Analytical (MDA) applications.

The OLAP techniques are used in Business Intelligence (BI), Relational Database, Data Mining, Business Reporting, Business Process Management (BPM), Financial Reporting, etc., to process large quantities of transaction data while avoiding large storage normally needed for this purpose.

These techniques eliminate the need for time consuming log scanning and tracking activities which tie up system resources and increase the information technology (IT) operating costs.

At the core of any OLAP system there is an OLAP cube (also known as "multidimensional cube" or a "hypercube"). It consists of numeric facts called **measures** that are categorized by **dimensions**.

Each measure can be thought of as having a set of **labels**, or meta-data associated with it. A dimension is what describes these labels; it provides information about the measure.

The measures are placed at the intersections of the hypercube, which is spanned by the dimensions as a vector space.

The usual interface to manipulate an OLAP cube is a matrix interface, like Pivot Tables in a spreadsheet program, which performs projection operations along the dimensions, such as aggregation or averaging.

It allows interactive, flexible (on-the-fly), and intuitive segmentation of security-related activities' tracking databases thus providing the user with invaluable business intelligence analysis data with clear graphical presentation for ease of interpretation.

With most security-analysis products, the system administrator faces a "needle-in-a-haystack" search task in order to analyze security breaches or other critical system activity.

Visualizer makes the whole process very resource efficient, simple and cost effective.

It presents a user-friendly JAVA-based Graphical User Interface (GUI), making the whole process a snap – simply point with the mouse, click and add the appropriate parameters to the filter section and a chart will be generated, in a matter of seconds, to tell the whole story in a glimpse.

Tweaking the analysis is also possible with simple mouse-clicks and the revised results will be presented immediately.



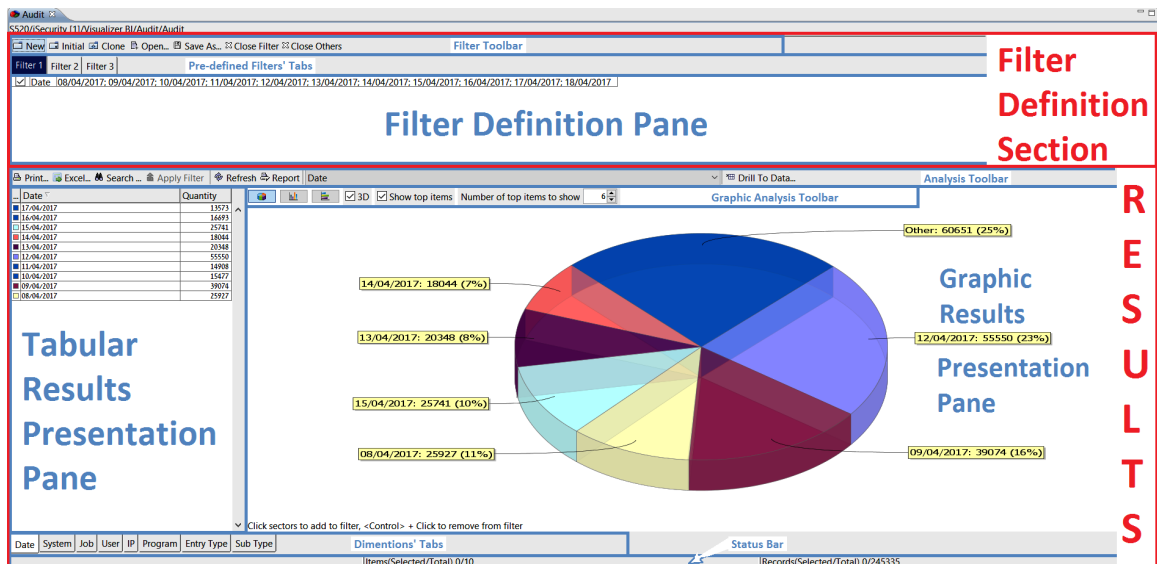
# The Visualizer Graphical User Interface (GUI)

Visualizer utilizes a single screen for defining the analysis rules and the presentation of its results.

This screen divides into two (2) main sections (marked with red frames on the figure ):

- The Filter Definition section, and
- The Results section.

Each section divides into toolbars, selection tabs and panes (marked with blue frames in the following figure) which will be described, from bottom up below.



## The Dimensions' Tabs



All **Dimensions** table (data fields) included in the analysis process are presented as tabs at the bottom-left side of the Tabular Results Presentation Pane.

A mouse click on any of these tabs define the leading criteria for the data screening filter and, thus, will also be updated in the Tabular Results Presentation Pane in the **Filter's Data Content Table's** header column.

All analyzed records which include valid data in the selected dimension (presented by the Tab) will be processed throughout the analysis procedure.

**NOTE:** Visualizer initiates with default filter definitions which present relevant data in the Graphical Results Presentation Pane, the Tabular Results Presentation Pane and the Filter Definition Pane and Selection Tabs. Please refer to section Initial Filter for further details.

## Tabular Results Presentation Pane

Following the Tab selection (setting the analysis pivot), all records matching the Tab's dimension (data field, criteria) will be added to the **Filter's Data Content Table** included in the Tabular Results Presentation Pane, in which each row represents an occurrence matching the Tab.

The left column of the table details the occurrence and the right column quantifies that occurrence.

The following figure demonstrates the **Table Presentation** in which the **Date Tab** was selected and quantities of occurrence are counted for each date matching the selection criteria.

The leftmost column shows relevant color for the occurrence as presented in the Graphical Results Presentation Pane.

The column to its right shows the items relating to The Dimensions' Tabs.

The rightmost column shows the number (quantities) of occurrences for each item row of the table.

For further analysis of the data, each (or a few) of the table's rows can be selected to create a new filter definition/combination, by holding down the keyboard's `Ctrl` button and clicking with the mouse on the row to be selected.

The new filter definition will also be updated in the Filter Definition Pane and Selection Tabs.

...	Date ▾	Quantity
■	17/04/2017	13573
■	16/04/2017	16693
■	15/04/2017	25741
■	14/04/2017	18044
■	13/04/2017	20348
■	12/04/2017	55550
■	11/04/2017	14908
■	10/04/2017	15477
■	09/04/2017	39074
■	08/04/2017	25927

**NOTE:** Visualizer works with a statistical file created as a batch process in the IBM i. Therefore, all dates listed in the **Date dimension** (set as the default option) in the **Data pane** will be from when the first entries were made to the system.

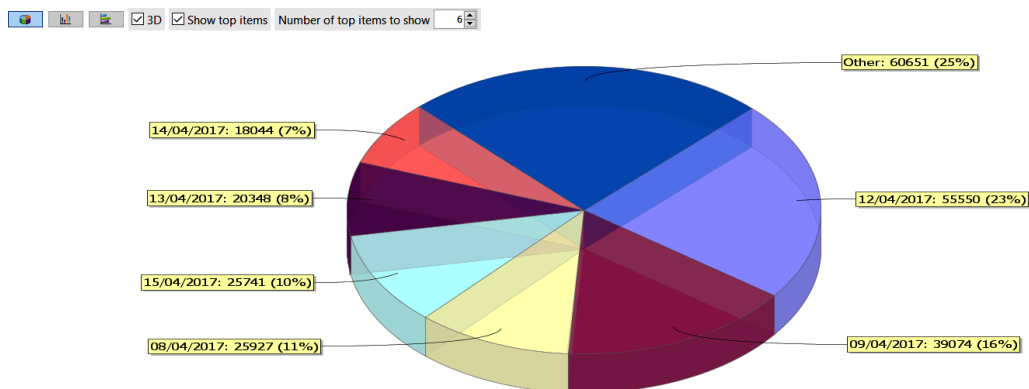
## Graphical Results Presentation Pane

To the right of the Tabular Results Presentation Pane, there is the Graphical Results Presentation Pane displaying the same analysis results but in a graphical format for ease of apprehending.

As in the Tabular Results Presentation Pane, for further investigation of the data, each of the graphic sections may be selected to create a new filter definition, by holding down the keyboard's **Ctrl** button and clicking with the mouse on the graph slice to be added to the filter definition.

The new filter definition will also be updated in the Filter Definition Pane and Selection Tabs.

**NOTE:** Visualizer, upon initiation, comes up with some default filter definitions, thus presents, immediately, some data in the Graphical Results Presentation Pane, the Tabular Results Presentation Pane and the Filter Definition Pane and Selection Tabs. Please refer to section Initial Filter for further details on the default values.



Click sectors to add to filter, <Control> + Click to remove from filter

## Graphical Analysis Toolbar

At the top left side of the Graphical Results Presentation Pane there is an additional toolbar used for the control of the graphical representation:



Its components, from left to right, are divided into two (2) groups:

### Group 1 – Chart Format

The purpose of the first group is to set the style of the chart.

It includes:



*Icon* – select Pie Chart presentation.



*Icon* – select Vertical Bar presentation.



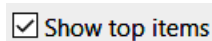
*Icon* – select Horizontal Bar presentation.



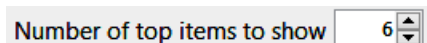
*Check box* – activate 3D presentation.

### Group 2 – Chart's Limits

The second group controls additional amount of items limitation for the filter. It includes:



*Check Box* – apply the limitation setup (see below).



*Spin Box* – set number of items for limitation.

**NOTE:** The above chart limit (Top) items refer to top (highest) quantities of items in the Filter's Data Content Table (rightmost column) included in the Tabular Results Presentation Pane.

## Analysis Toolbar

Above the Tabular Results Presentation Pane and the Graphical Results Presentation Pane there is an additional toolbar for different tasks on data presented in the Graphical Results Presentation Pane:

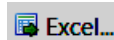
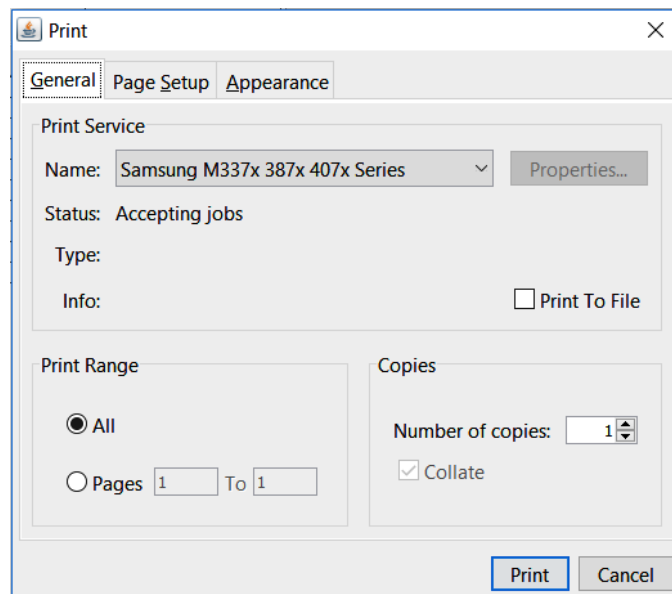


It includes:



*Button* – print the table of analysis results.

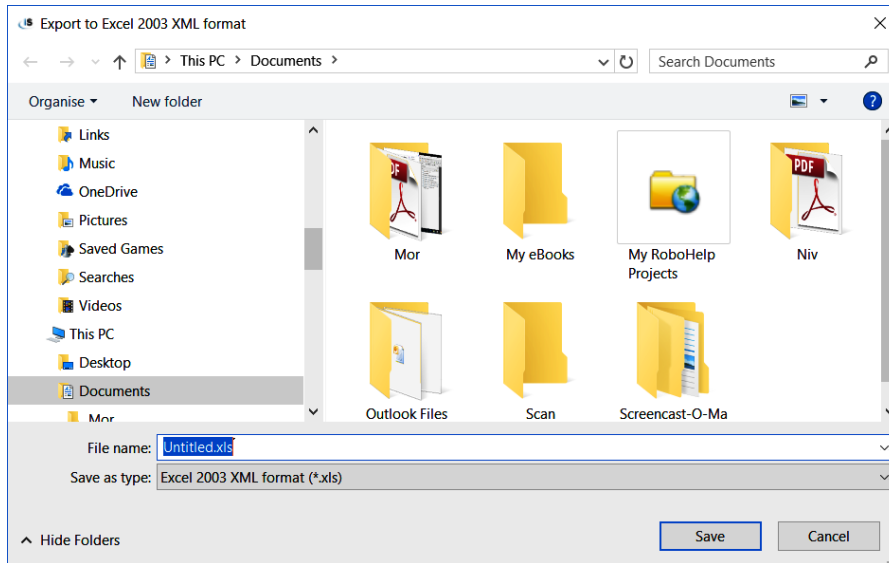
Clicking with the mouse on the **Print Button** will bring up the **Print Dialog Box** for printer setup, as demonstrated below:



*Button* – export analysis results to Excel spreadsheet file.

Clicking with the mouse on the **Excel Button** will bring up the **Export to Excel 2003 XML Format Dialog Box** where the Excel file name and storage location need to be set.

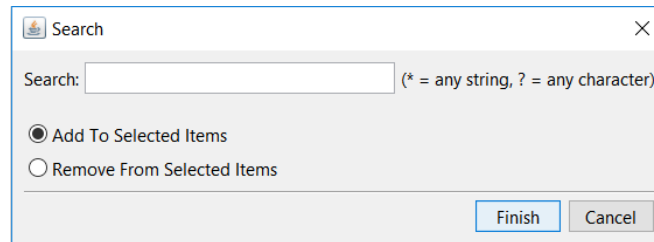




#### Search ...

*Button* – search for text within the left column of the Filter's DataContent Table.

Clicking with the mouse on the **Search Button** will bring up the **Search Dialog Box** where the text to look for can be entered. Select if the found text should to be added or removed from the selected items.



#### Apply Filter

*Button* – apply changes to the filter's definitions.

Clicking with the mouse on the **Apply Filter Button** will remove items not marked for selection.

#### Refresh

*Button* – refresh the analysis results.

Refresh causes all data to be re-read from the server and all analysis to be re-applied.

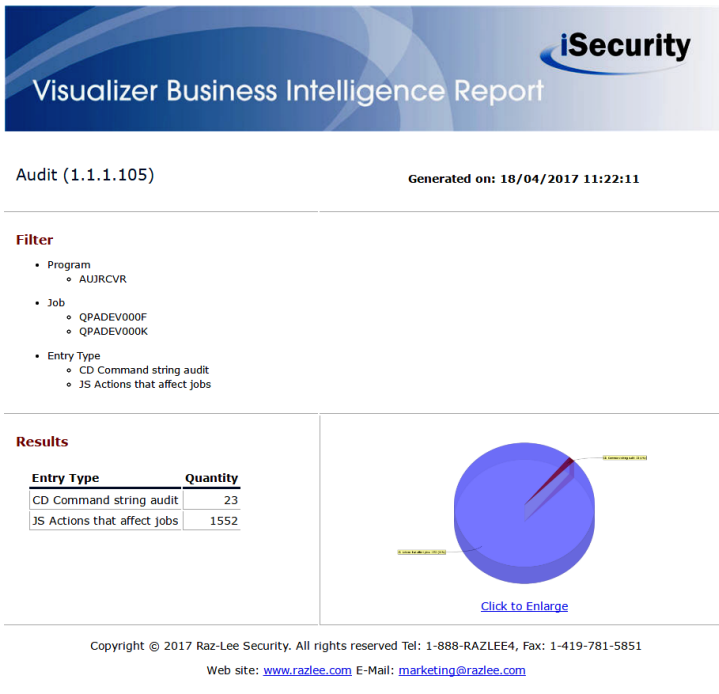
#### Report

*Button* – for generating a report (in HTML format), as demonstrated on page 51.

#### Date

*Combo box* – selection of the dimensions included the graph.

Selecting dimensions utilizing this combo box is equivalent to selection via The Dimensions' Tabs.



Audit (1.1.1.105) Generated on: 18/04/2017 11:22:11

**Filter**

- Program
  - AUJRCVR
- Job
  - QPADEV000F
  - QPADEV000K
- Entry Type
  - CD Command string audit
  - JS Actions that affect jobs

**Results**

Entry Type	Quantity
CD Command string audit	23
JS Actions that affect jobs	1552

[Click to Enlarge](#)

Copyright © 2017 Raz-Lee Security. All rights reserved Tel: 1-888-RAZLEE4, Fax: 1-419-781-5851  
Web site: [www.razlee.com](http://www.razlee.com) E-Mail: [marketing@razlee.com](mailto:marketing@razlee.com)

#### Drill To Data...

*Button* – access the full log data, based upon the filter settings.

Clicking on the **Drill To Data Button** with the mouse will bring up the **Drill to [Application Name] Log Dialog Box** where the time limits for analysis may be set. Selecting **Prompt on every activation** may also be set.

## Status Bar

Below the Tabular Results Presentation Pane and the Graphical Results Presentation Pane, at the bottom of the screen, there is a status bar representing the numbers of items and records involved in the analysis process:

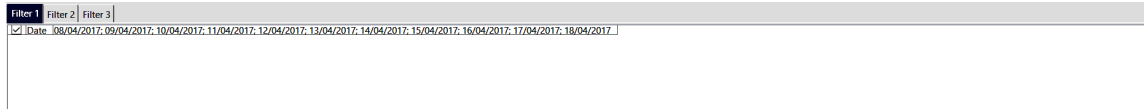
Items(Selected/Total) 0/10	Records(Selected/Total) 0/245335
----------------------------	----------------------------------

**NOTE:** Visualizer, upon initiation, comes up with some default filter definitions, thus presents, immediately, some data in the Graphical Results Presentation Pane, the Tabular Results Presentation Pane and the Filter Definition Pane and Selection Tabs. Please refer to section Initial Filter on page 63 for further details on the default values.

**Items** (units of information in the analyzed file or number of rows in the Filter's Data Content Table included in the Tabular Results Presentation Pane) are displayed on the left side of the bar, while **records** (entries to the analysis process) – on the right. In both cases the display presents selected (value) vs. total (value).

## Filter Definition Pane and Selection Tabs

Above the Tabular Results Presentation Pane and the Graphical Results Presentation Pane there is a **Filter Definition Pane** where filter definitions (or limits) are displayed.

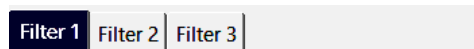


There is no limit to the number of filters that may be defined for each analysis job, but only one of them may be active at a time.

Numerous filter setups can be defined using the tabs above the **Filter Definition Pane**.

These tabs enable ease of navigation between several pre-defined filters for the analysis job.

The default (see paragraph Initial Filter below) number of Tabs (Filters) is three (3).

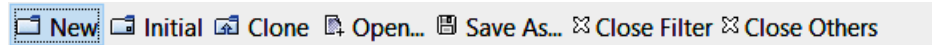


**NOTE:** Visualizer, upon initiation, comes up with some default filter definitions, thus presents, immediately, some data in the Graphical Results Presentation Pane, the Tabular Results Presentation Pane and the Filter Definition Pane and Selection Tabs. Please refer to section Initial Filter on page 63 for further details on the default values.

Visualizer changes the display dynamically in accordance with the user's selection of new criteria during the process of analysis.

## Filters Toolbar

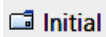
Above the Filter Definition Pane and Selection Tabs there is a general **Filters Toolbar** allowing setting up the filters defined:



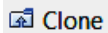
It includes:



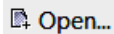
Creation and opening of a new filter definition (and thus – a new tab in the **Pre-Defined Filter Tabs**).



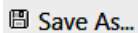
Re-initiation of the default Initial Filter definitions.



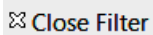
Duplication of currently opened filter including initiating a new tab.



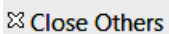
Opens a previously-saved filter from the filters' library.



Saves the current filter definition as a new filter into a library.



Closes (deletes) the filter in use.



Closes (deletes) the filters not in use.

## General Issues

The Visualizer GUI behaves just like any other Windows application:

- Its windows can be resized, moved closed and re-opened.
- Selection of items (all types) is done by clicking left mouse button on the item,
- Multiple items can be selected by holding down the keyboard's button and clicking with left mouse' button,
- Selection of multiple sequential items can be chosen by holding down the button,

## Initial Filter

To accelerate its initiation, Visualizer (as an iSecurity component, see more details in Chapter 4 Introduction to the iSecurity Authority InspectorChapter 4 Introduction to the iSecurity Authority Inspector) launches with a number of default filter definitions.

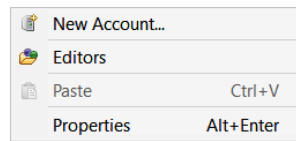
The first screen presented shows initial data in the Graphical Results Presentation Pane, the Tabular Results Presentation Pane and the Filter Definition Pane and Selection Tabs.

The defaults are three (3) identical pre-defined filters; each refers to the **Date** field and includes only ten (10) occurrences.

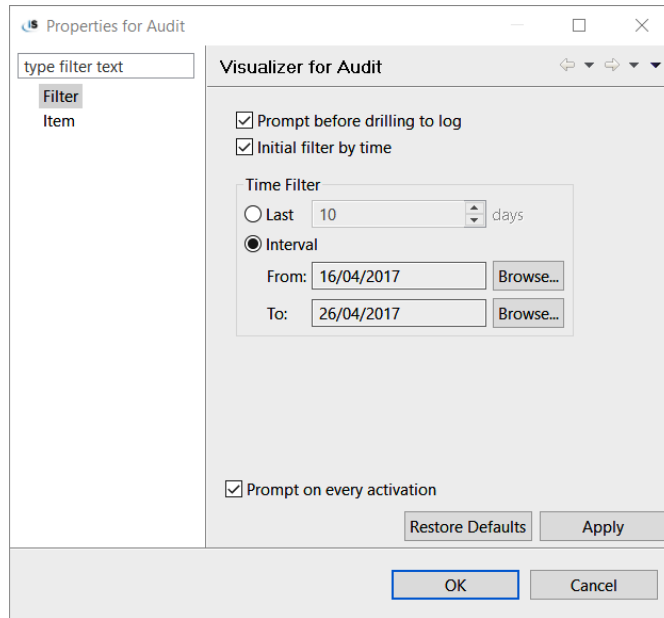
This way, the data set for analysis is very limited and the results are presented promptly upon initiation.

These defaults can be altered by:

1. Right-click the mouse on the application name (Audit in this example) in the **Navigator Pane** (left side of the screen) to open the roll-down menu:



2. Select the **Properties** menu item (with mouse left-button click or, alternatively, by pressing the **Ctrl** and **Enter** keys of the keyboard simultaneously) to bring up the **Properties for Audit Dialog Box** presented below:



3. Click the mouse on the **Filter menu line** in the left side of the **Properties for Audit Dialog Box**.

The **Properties for Audit Dialog Box** allows setting of default values of the Initial Filter by:

- Selecting the option for **Prompt before drilling to log**,
- Selecting and limiting default filter by time, either for a set number of last days (before activation) or by setting a specific time-frame,
- Selecting if this default setting dialog box will automatically prompt upon activation.

Once the default options have been set, there is a need to save them by clicking with the mouse on the **Apply Button** or switching them back to the factory defaults by clicking on the **Restore Defaults Button**.



## Working with the Visualizer

---

The recommended strategy for using Visualizer to analyse security related activities is to successively define filters (queries) to present data views as defined by the filters.

These data views include specific events as well as the system data related to these events.

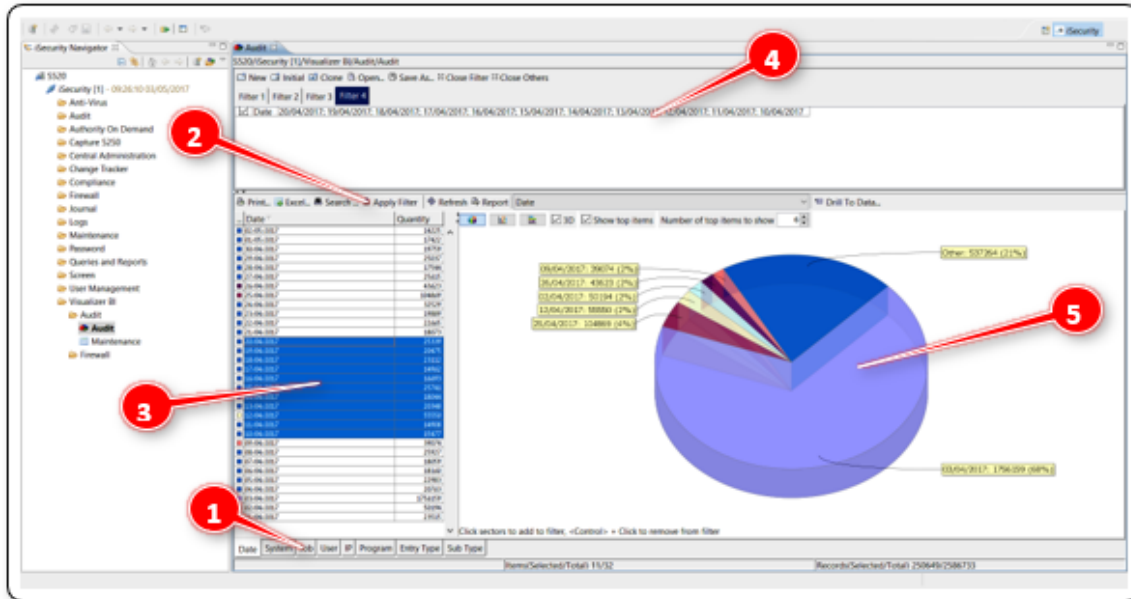
Let's look at an example of a potential security threat using Visualizer for Audit. The scenario is:

*There is a suspected security break-in by an unknown user who seems to attempt to change another user's password or, alternatively, to tamper with another user's profile data and execute operations which might be destructive to the system.*

*Known facts which supports the exposure of this threat and the perpetrator, are:*

- *These actions took place within some known timeframe(s),*
- *The suspected users are (mostly) known,*
- *Their working IP is also (mostly) known,*
- *The system in use is known, and*
- *The operation used by the suspected users is also known.*

## Setting up Filters



Since the timeframe of the suspected intrusive events (occurrences) is known, filtering will commence with limiting the analyzed data to this timeframe.

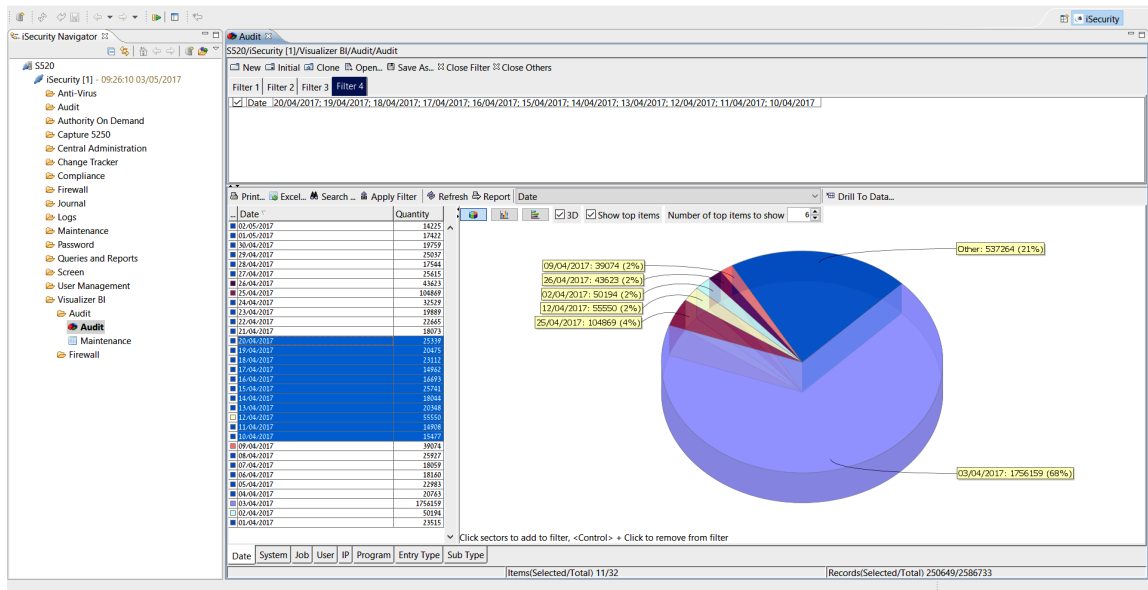
For this example – the events took place from April 10<sup>th</sup>, 2017 till April 20<sup>th</sup>, 2017.

This time-window is selected, in The Dimensions' Tabs **Date Tab** (field) by clicking on the first date (10-4-2017), holding down the keyboard's **Shift** key and clicking with the mouse again on the second date (20-4-2017).

The result will be a highlighted timeframe as demonstrated (see ③) in the figure Setting up Filters.

Clicking on the **Apply Filter Button** (②) in the figure Setting up Filters) in the Analysis Toolbar will filter the presented data by the selected timeframe only.

This will affect the Tabular Results Presentation Pane (see ③ in the figure Setting up Filters), the Graphical Results Presentation Pane (see ⑤ in the figure Setting up Filters), and the Filter Definition Pane and Selection Tabs (see ④ in the figure Setting up Filters). The resulting screen is presented in the figure below.



At this early stage of setting up the filters, there is no point in investigating the results at this point in the process. But, since the dates of occurrences were established as a base for drilling into the data, the first selection of the **Date Tab** (data field) turns it into a pivot-like factor that will serve as the basis for our investigation.

Another known factor which will support the analysis of the occurrences is the IBM i system used for generating the occurrences. For the sake of this example, the system name used for generating the occurrences is S520. Clicking on the **System Tab** in the Tabular Results Presentation Pane will filter the events by the system name and enable selecting S520 as the working filter for the investigation. As before, clicking on the **Apply Filter Button** in the Analysis Toolbar at this point in time will filter the presented data to display only events.

Another known factor which may be used is the network IP address of the initiated event. In this example, the IP addresses range is 1.1.1.xxx (i.e. specific department in the organization). Clicking on the **IP Tab** in the Tabular Results Presentation Pane will present all IP addresses involved during the timeframe and under the specific system set before. As with Date above, the range of IP addresses covering 1.1.1.xxx should be highlighted in the Tabular Results Presentation Pane and will be included in the filter.

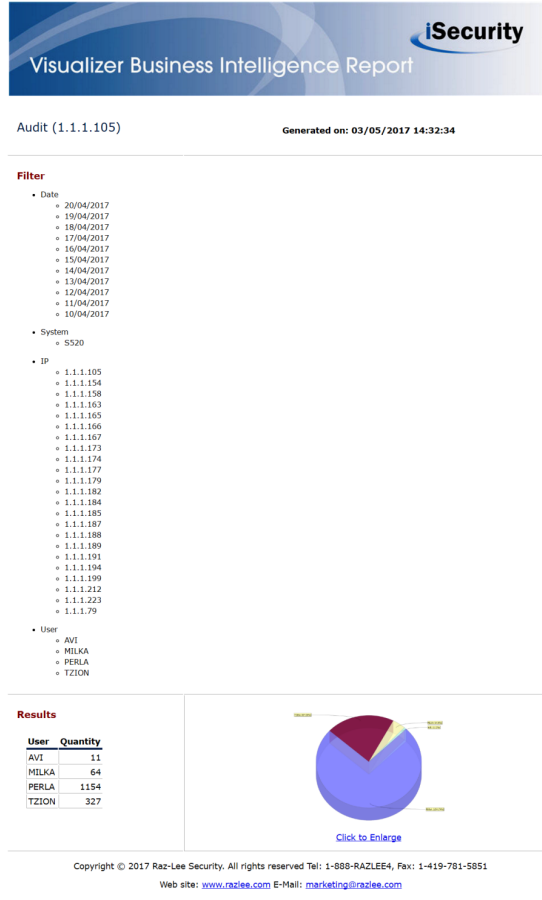
Now that all [Known Facts](#) were included in the filter, it is time to search for the suspected users – clicking with the mouse on the **User Tab** in the Tabular Results Presentation Pane will present all users that fit into the above progressively built filter. Since some of the filter-matching users are undoubtedly not suspicious, they can be eliminated from the filtering process by marking (highlighting) suspicious users only. For that purpose, click with the mouse on the first suspected user, hold down the keyboard's **Ctrl** key and keep clicking with the mouse on all other names. Mouse clicking on the **Apply Filter Button** in the Analysis Toolbar at this point in time will leave only the marked users in the filter and on the display.

Up to this point, Visualizer filters the investigated database which includes only the users who were active within the given timeframe and used a specific system, from a specific IP address range and were declared suspicious. The investigation may go further, by slicing **Entry Type** and **Program** in a similar fashion as described above. In the **Entry Type Tab** it makes sense to filter operations like **Create Object** to filter only the suspected user who used **Create Object** operation to alter the **User Profile**.

Once these were filtered, clicking with the mouse on the **Program Tab** will reveal which program(s) were incorrectly or erroneously used to build a new **Object**. These programs were abnormally used to alter the User Profile(s). Highlighting any of them and going back to the **Users Tab** will reveal the users who are most likely the sabotaging users. They fit all criteria used for filtering the data.

# Generating Reports

When the analysis is complete, it is possible to view the results as a report in printable HTML format. The report for the above example looks as follows:



# Chapter 4 Introduction to the iSecurity Authority Inspector

---

## Foreword

---

**NOTE:** It is mandatory to read Chapter 3 Introduction to iSecurity Visualizer before reading Chapter 4 Introduction to the iSecurity Authority Inspector.

Authority Inspector is based on the iSecurity Visualizer product and as such most explanations were presented in Chapter 3 Introduction to iSecurity Visualizer (see page 46).

The main differences between Visualizer and the Authority Inspector are:

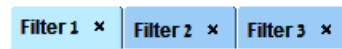
- **Databases** – Authority Inspector uses IBM's Authority Collection database file (QSYS2/AUTH\_COL) for analysis while Visualizer uses Raz-Lee's statistical database file (different for each Visualizer application, i.e. Visualizer for Audit, Visualizer for Firewall, etc.) created by the Visualizer based upon the system's log files.

**NOTE:** The above does not apply to The Demo Mode of the Authority Inspector which uses a pre-populated database for demo/evaluation purpose only.

- **Installation** – Authority Inspector has its own installation procedure, utterly different to other Visualizer applications.
- **Graphical User Interface (GUI)** – Authority Inspector look-and-feel is slightly different from Visualizer in terms of:
  - The graphic elements are slightly different since Authority Inspector is a Java based standalone application while Visualizer is an Eclipse platform based embedded application.

- The launching screen is slightly different and includes a The Demo Mode option.
- There is an additional **Data Pane** at the right-bottom side of the screen (within the **Results Pane**) allowing for more drill-down options.
- As a result of adding the above-mentioned **Data Pane**, three (3) essential buttons were added to the **Analysis Toolbar** (compared with the Visualizer **Analysis Toolbar**, see Analysis Toolbar page 56).
- **The Status Bar** – Now also include presentation of the **Field** selected as pivot as well as presentation of the number of records included (and analyzed) in the **Data Pane**.
- **The Filters Toolbar** was changed and does not include the **Close Filter** and the **Close Others Buttons**.

Instead, the **Filter Tabs** in the **Filter Definition Pane** include remove marks (x) which, upon click, perform the same function as the **Close Filter Button**:



- Some **Fields' data** were mapped – to ease understanding their content.

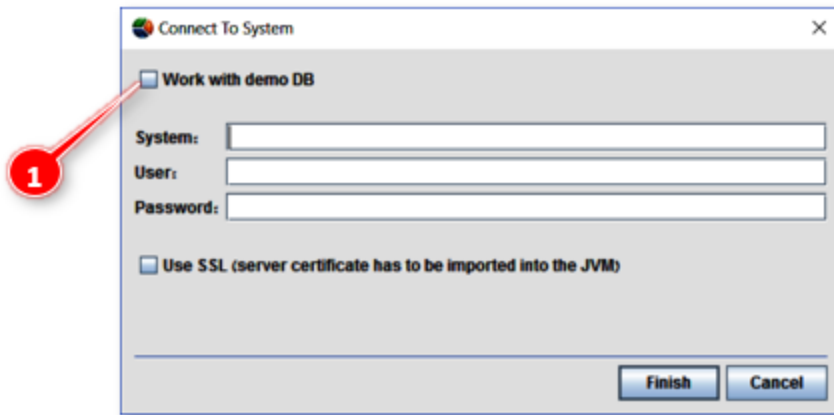
The following paragraphs will detail these dissimilarities and their functionality based on the assumption that the user is at least somewhat familiar with the Visualizer (detailed in Chapter 3 Introduction to iSecurity Visualizer).



## The Demo Mode

The **Connect to System Dialog Box** of the Authority Inspector include the **Demo Mode** option Check Box (1) in the figure below.

This option allows usage of an embedded database for demo/evaluation analysis.



**NOTE:** Marking the **Demo Mode Check Box** also means that there is no need to fill-in the **System**, **User** and **Password** fields and that the **Use SSL Check-box** has no use.

Selecting **Demo Mode** is done by marking the Check Box and clicking on the **Finish Button** immediately after.

The Authority Inspector **Main Screen** will open as demonstrated in the figure below.

The **Demo Mode** is similar to normal operation and is described in detail in Chapter 6 Using the Authority Inspector.

Authority Inspector - Part of Security Suite by Ras-Lee Security - connected to DEMO

File Help

New Initial Close Open... Save As...

Filter 1 x Filter 2 x Filter 3 x

Work with... Select Values... Refresh Apply Filter Data Area... Cancel Excel...

Collected For User

Collected For User	Quantity
ALEX3	397
DB	743
RAZLEELOF	427

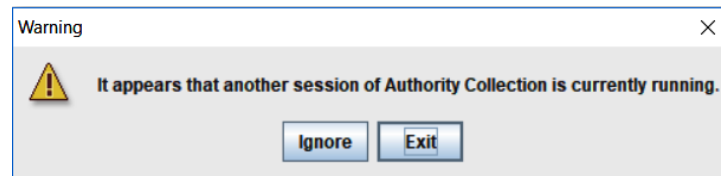
Click on chart items to add. Cb-Click to remove

Collected For User	Object	Library	Type	Authority Check Successful	Check Any Authority	Required Authority	Current Authority	Authority Source	Current Adopted Authority	Adopted Authority
RAZLEELOF	AUCMER	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	QUSRYSYS	GSYS	LIB	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	RIVDTAA	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	AUCNDIR	SMZDITA	FILE	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	SMZDITA	GSYS	LIB	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	DBEPWDR	SMZB	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	ENGSSIS	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	ALMDSQPR	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUFGSCOUR	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	QVNDQBF	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	JRREL	SMZJ	DTAARA	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUSELR	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUOQGR	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	WVNSRSDQBF	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	RLGZ	SMZDITA	FILE	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	GD	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	AUCBYR	SMZC	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUJYMR	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	SNRBYR	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	QDPL	GSYS	LIB	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	QSEFWOR	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	CALL	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUSELQFM	SMZA	FILE	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUVAISR	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	DLTJOB	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	CAK	SMZC	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUDATCR	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	DISPALOG	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	SMZDITA	GSYS	LIB	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUSELRPM	SMZA	FILE	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	AUSGDM	SMZC	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	GSDQOPN	SMZSYS	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	ALMDSGM	SMZA	FILE	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUQNDQPM	SMZA	FILE	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	GSNM.GD	SMZJ	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUDOUTR	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	AUCJID	SMZDITA	DTAARA	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	QGENZDT	GSYS	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	SMZDITA	GSYS	LIB	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUSROUTR	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	DISPALOG	SMZA	PGM	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
RAZLEELOF	AUSELR	SMZA	PGM	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	JRREL	SMZJ	DTAARA	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	QASQRESL	GSYS	FILE	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
DB	DBPWDR	SMZDITA	FILE	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	RIVDTAAL	GSYS	CMD	Yes	Specific	-	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB
ALEX3	QKQZLQZ	SMZJGXA	CLZ	Yes	Any	HALL	HALL	USER-ALLOUJ	HALL	ADOPTED-ALLOB

Field: Collected For User      [Items Selected: Total] 6/3      [Records Selected: Total] 6/427      [Data Table: 288 records]

## Single Session Operation

The Authority Inspector software is built for single session operation. Therefore, in case the Authority Inspector is re-triggered while an earlier session is already active, the following Message Box will pop-up:



It is recommended to click on the **Exit Button** and terminate the second session.

## Databases for Analysis

---

The database for the Authority Inspector is IBM's Authority Collection repository file (QSYS2/AUTH\_COL) while other Visualizer applications create their own statistics database for analysis, derived out of the syslog files as follows:

**NOTE:** The above does not apply to The Demo Mode of the Authority Inspector which uses some embedded database for demo/evaluation purpose only.

## Installing the Authority Inspector

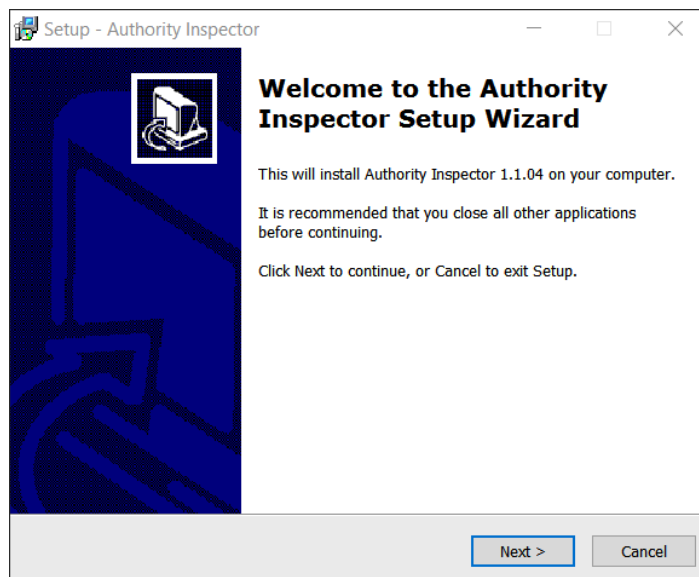
---

The process of installing the Authority Inspector is a straightforward job similar to the installation of most Windows applications.

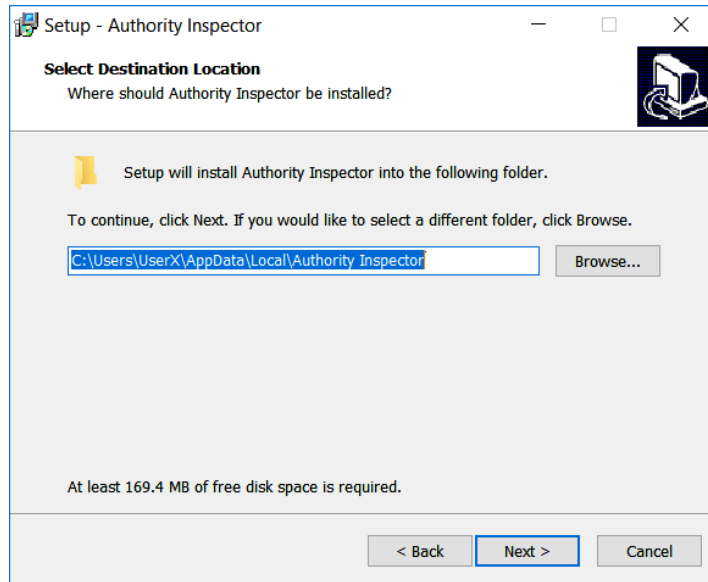
The installation steps are:

1. Double-click with the mouse on the authority-inspector-setup.exe program provided by Raz-Lee and wait for the **Welcome to the Authority Inspector Setup Wizard Message Box** (see screen capture on the page ) to pop-up.

The installation process may be terminated at this stage by clicking with the mouse on the **Cancel Button**.



2. Mouse click on the **Next> Button** to prompt the **Select Destination Location Dialog Box**:



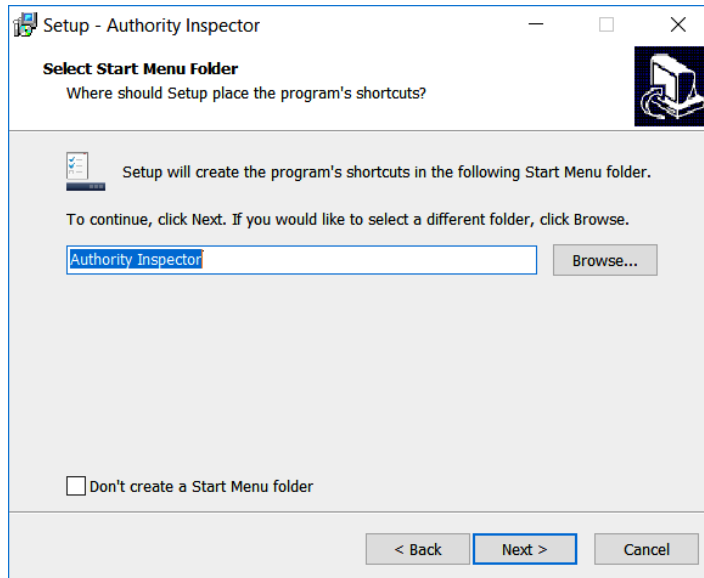
The default location is set to the user's folder and may be manually altered to another location.

This is done either by typing-in the exact path, or by browsing with Window's File Explorer application (click on the **Browse Button** for that purpose).

The installation process may be terminated at this stage by clicking on the **Cancel Button**.

There is also a possibility to go one step back by clicking on the **<Back Button**.

3. Once the location is set, mouse click on the **Next> Button** to prompt the **Select Start Menu Folder Dialog Box** and set Windows' Start Menu location for the Authority Inspector sub-menu:



The default menu name is set to Authority Inspector but may be manually altered to another name:

- Either by typing-in the alternative name, or
- By browsing to find another name; click on the **Browse Button** as necessary.

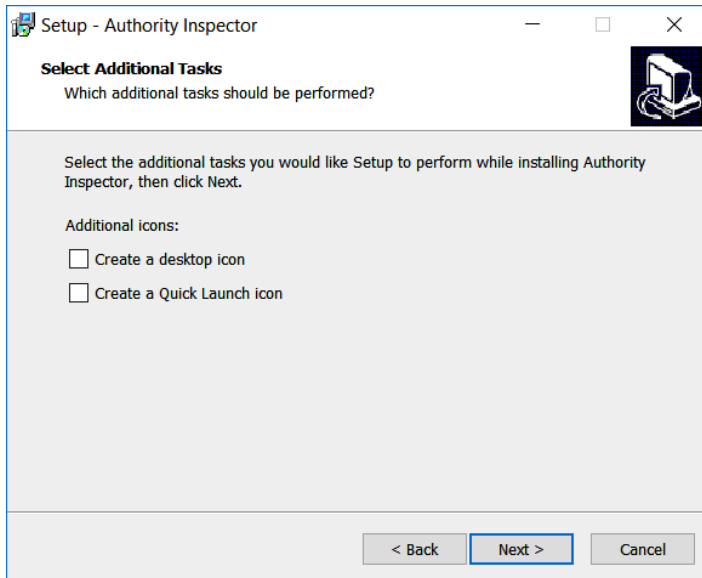
A Check Box is provided to skip the creation of a **Start Menu Folder** step.

The installation process may be terminated at this point in time by clicking with the mouse on the **Cancel Button**.

There is also a possibility to go one step back by clicking with the mouse on the **<Back Button**.

4. Once the **Start Menu Folder** is set, click with the mouse on the **Next> Button** to prompt for the **Select Additional Tasks Dialog Box** to set two (2) additional options:
  - Creation of a **Desktop Icon**, and
  - A **Quick Launch Icon**.

Each icon option may be selected by marking a check box.



The installation process may be terminated at this stage by clicking with the mouse on the **Cancel Button**.

There is also a possibility to go one step back by clicking with the mouse on the **<Back Button**.

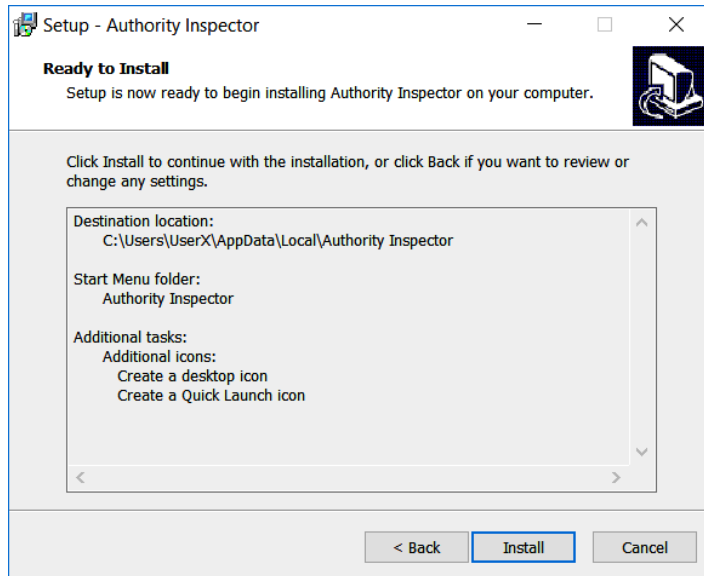
The following program launching icon will appear on the desktop soon after the installation, if the **Create a desktop Icon Check Box** is marked.



The same icon, although smaller, will be included in the computer's **Quick Launching Tray (Pinned Taskbar Buttons** in Windows 7 and above) if the **Create a Quick Launch Icon Check Box** is marked.

5. Once all the above installation data is set and following a click with the mouse on the **Next> Button**, a **Ready To Install Dialog Box** will pop-up:





It summarizes the above given setup data (destination, Start Menu, icons, etc.) for confirmation.

Verify and setup data and click on the **Install Button** to continue.

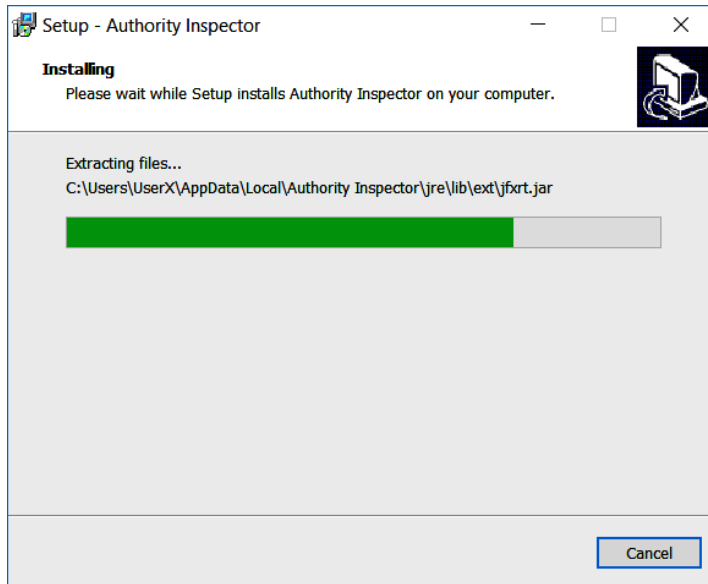
In case there is a need to correct any of above; a **<Back Button** is provided to navigate back to one of the above described dialog boxes for correction.

The installation process might be terminated at this stage by mouse clicking on the **Cancel Button**.

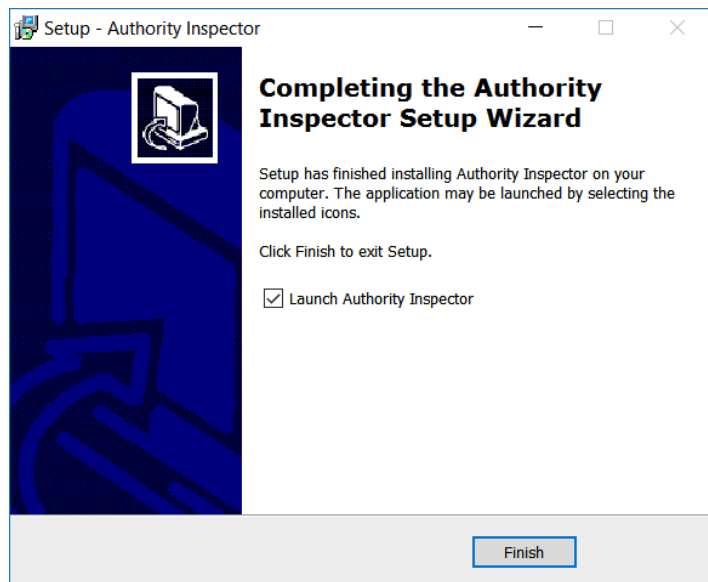
In case all setup data is correct, click with the mouse on the **Install Button** to initiate the installation procedure.

6. An **Installing Dialog Box** with a **Progress Indicator** will appear for the reminder of the installation process.

The installation process might be terminated at this stage, by mouse clicking on the **Cancel Button**.



7. Immediately after the completion of the installation procedure, a **Completing the Authority Inspector Setup Wizard Dialog Box** will pop-up.

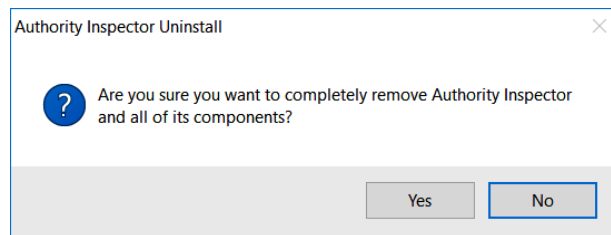


The **Authority Inspector** may be selected for launching immediately by marking the **Launch Authority Inspector Check Box**. Click with the mouse on the **Finish Button** to exit the installation program.

## Uninstalling the Authority Inspector

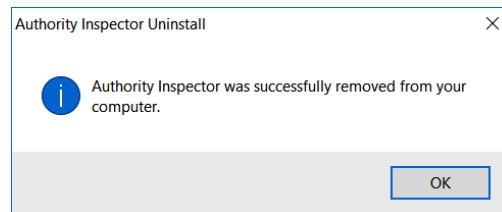
To uninstall Authority Inspector, perform any of the following:

- Browse to the Authority Inspector **Start Menu** directory (default location – C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ Authority Inspector) and double-click with the mouse on the **Uninstall Authority Inspector Shortcut**. Since this is a drastic action, a Dialog Box will pop-up to confirm the action.



Clicking on the **No Button** will cancel the uninstall command while clicking on the **Yes Button** will initiate the uninstall operation.

Once the uninstall operation is complete, the following Dialog Box will pop-up to inform completion of this operation:



Click on the **OK Button** to terminate the uninstall session.

Other uninstalling options may be:

- Browse to the Authority Inspector installation directory (default location – C:\Users\[**UserName**]\AppData\Local\Authority Inspector) and double-click with the mouse on the **unins000.exe application program**.
- Select the PC's **Settings menu** (or **Control Panel** in older Windows OS installations), select the **Apps & features menu option** (or the **Add or Remove Programs** option in Control Panel) and uninstall Authority Inspector from there.

- Depending on the Windows OS version installed; click with the mouse on the **Windows Start Icon** (bottom-left corner of the screen) to reveal the main menu and then right-click the mouse on the Authority Inspector menu option to open its sub-menu where an un-install menu option is available.

## Graphical User Interface (GUI)

---

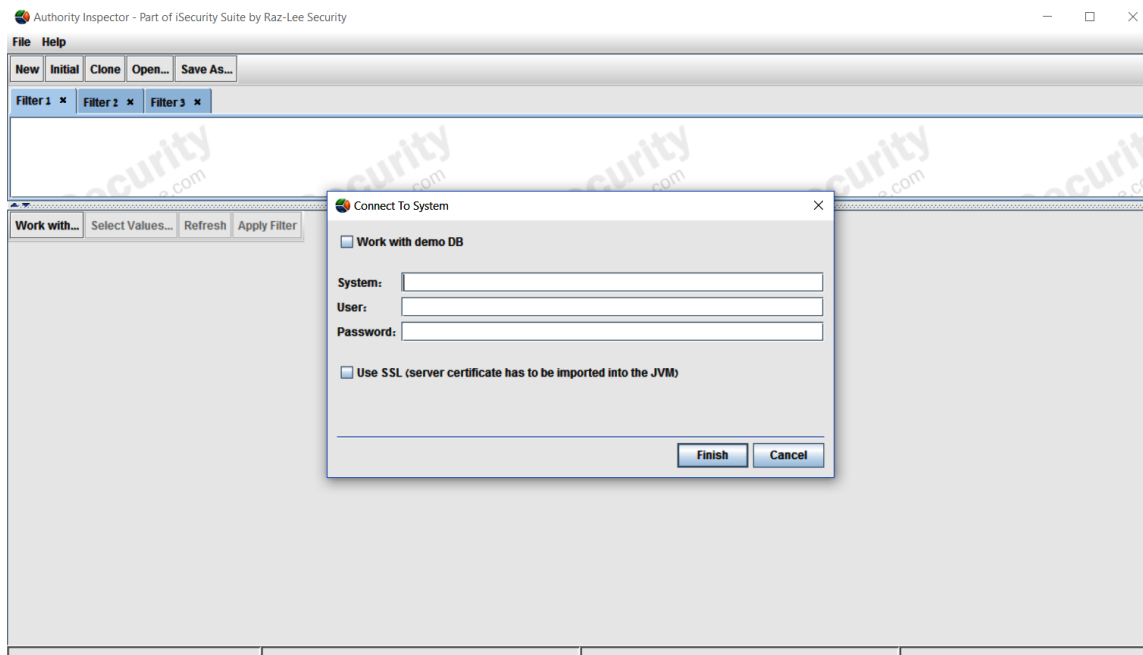
As mentioned before; the Authority Inspector Graphical User Interface (GUI) look-and-feel is slightly different from Raz-Lee's Visualizer.

This section details the dissimilarities and focus on the GUI's operational aspects while Chapter 5 Configuring the Authority Inspector details how to use it.

## The Launching Screen

Every time Authority Inspector is launched (except for the first time), the launching screen will include a **Connect to System Dialog Box** on top of data-free **Main Screen**:

**NOTE:** Launching Authority Inspector for the first time is a special configuration case detailed in section First-Time Launching of Authority Inspector.



## Connect to System Dialog Box

The **Connect to System Dialog Box** controls which data file is used for the Authority Inspector analysis process:

- The embedded **demo DB** data file (see details in The Demo ModeThe Demo Mode), or
- A real Authority Collection data file (IBM's Authority Collection database file – QSYS2/AUTH\_COL).

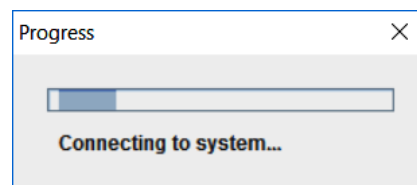
Usage of the real IBM QSYS2/AUTH\_COL file for authorities' analysis requires:

- Typing-in the System's **IP address** (or the computer's **System Name**)
- Providing the **User name** and **Password**.



There is also an option to utilize **SSL** (Secure Sockets Layer; a cryptographic protocol providing communications security over a computer network) by marking the checkbox provided for this purpose on the **Connect to System Dialog Box**.

Clicking on the **Finish Button** will invoke connection to the server (AS/400) for fetching the data for analysis. During the period of time required for this operation, a **Progress Indicator** will report the operation's progress:



## Running Authority Inspector in SSL Mode

In computer networks where high communication security is mandatory, Secure Sockets Layer (SSL) protocols are used to provide privacy and data integrity between two communicating computer applications. Such protocols may be used for Authority Collection analysis applications like the Authority Inspector.

**NOTE:** Prior to initiating the following procedure, the IBM i system **must** be configured to work with SSL protocols and the Sysadmin **must** activate web server on the IBM i, utilizing the command: STRTCPSVR SERVER (\*HTTP) HTTPSVR (\*ADMIN) to create an interface for the User.

1. Enter the address in the Address Bar as follows: `http://[servername/IP]:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0`.



**Digital Certificate Manager** 

Select a Certificate Store

Expand All Collapse All

- Create Certificate
- Create New Certificate Store
- **Install Local CA Certificate on Your PC**
- ▶ Manage User Certificates
- ▶ Manage CRL Locations
- Manage LDAP Location
- Manage PKIX Request Location

Return to IBM i Tasks

Secure Connection



5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1, 5761-SS1, 5770-SS1 (C) Copyright IBM Corporation 1997, 2009  
All rights reserved.  
US Government Users Restricted Rights -  
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.  
Licensed Materials - Property of IBM

 Contains software from RSA Data Security, Inc.

Get Started

2. Mouse click on the **Install Local CA Certificate on Your PC Menu** option:
3. Mouse click on the **Copy and paste certificate Link** to open the Certificate data page.





Select a Certificate Store

Expand All Collapse All

- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC**
- Manage User Certificates
- Manage CRL Locations
- Manage LDAP Location
- Manage PKIX Request Location
- Return to IBM i Tasks

Secure Connection

#### Install Local CA Certificate on Your PC

##### To install (receive) the certificate on your browser:

Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.

[Install certificate](#)

##### To copy and paste the certificate to a file on your PC:

If you need the Certificate Authority (CA) certificate for a non-browser application such as Client Access Express or IBM Personal Communications, choose the Copy and paste certificate link. Use the online help provided here and in the appropriate application for information about working with your certificate file. Click the following link to copy and paste the certificate into a file on your PC.

[Copy and paste certificate](#)

OK

4. Copy the Certificate's texts presented and paste it into Microsoft Notepad.
5. Save the Notepad file with a file name (i.e. ca.txt), to the Authority Inspector installation location (default location: C:\Users\[Username]\AppData\Local\Authority Inspector).
6. On the PC, open the Command Prompt and change the directory to the Authority Inspector installation location by typing-in: cd\ C:\Users\[Username]\AppData\Local\Authority Inspector.
7. From the same location use the Java Keytool to import the certificate into a trust list by issuing the following command: jre\bin\keytool -import -v -trustcacerts -alias <aliasName> -file ca.txt -keystore trustlist (the alias is an option).

This will create a file called **trustlist** and while processing the above command; it will prompt the user to establish a password for this file.

## Providing Trust Store Data from Command Line

From the PC's Command Prompt, set to the Authority Inspector installation location (default: C:\Users\[Username]\AppData\Local\Authority Inspector), type-in the following command:

```
authority-inspector.exe -vmargs -Djavax.net.ssl.trustStore= trustlist -Djavax.net.ssl.trustStorePassword=pwd.
```

Replace trustlist and pwd with the User's system parameters (same parameters used in [Running Authority Inspector.htm](#)). The **Trustlist** parameter is the absolute path to the file itself including file name (i.e. c:\...\trustlist) but if this file resides on the Authority Inspector installation location, there is no need to type the path.

---

**NOTE:** More details on IBM's Digital Certificate Manager (DCM) may be found in [DCM – FAQ and Common Tasks](#).

---

## The Fields' Tabs

IBM's Authority Collection database file (QSYS2/AUTH\_COL) includes sixty-three (63) data fields. Only some of these data fields will be used in the specific analysis tasks.

**NOTE:** In business intelligence terminology the **Fields** are referred to as **Dimensions**.

Unlike the Visualizer, the Authority Inspector has no **Fields' Tabs** at all but, instead, uses the **Work with Button's Drop-Down Menu** for the same purpose of selecting which data field to work with as a pivot for the analysis. This **Drop-Down Menu's Fields** are used in the same way as The Dimensions' Tabs are used in the Visualizer.

The default **Fields** may be altered, both in content (which fields out of the 63 will be included) and in their order of presentation, utilizing the Authority Inspector **Main Menu's File** option and **Initial Authority Collection fields and order link**.

See details in section The Main Menu – File Sub-Menu .

## The Data Pane

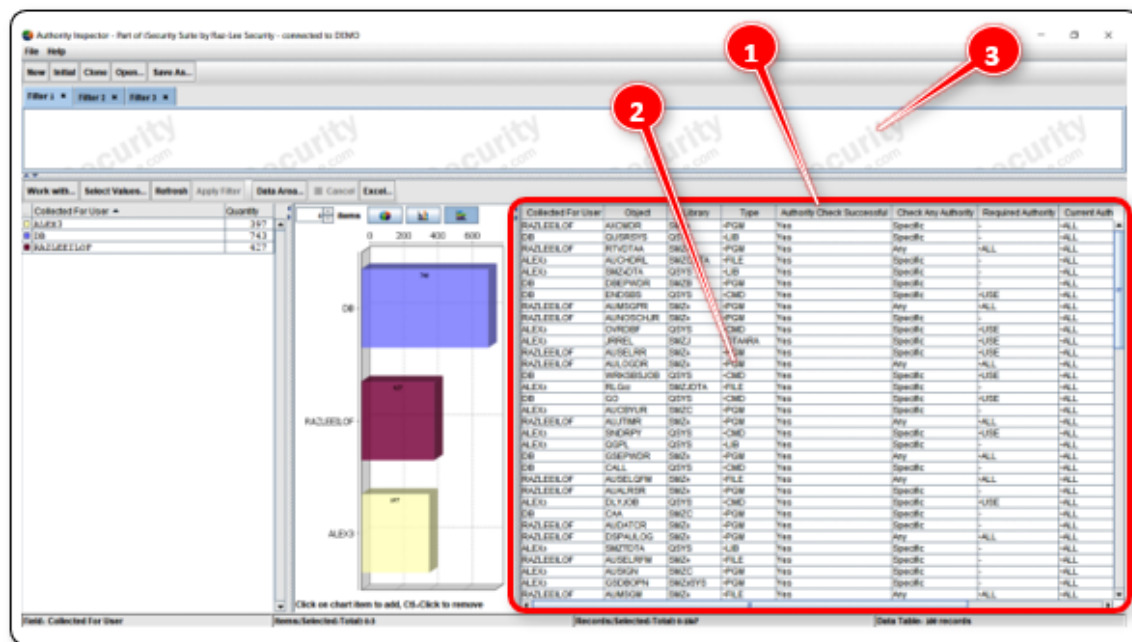
The above mentioned Fields, represented by the **Data Pane Table Titles** (marked ① in the [following](#) figure), are detailed in the **Data Pane** (marked ② in the [following](#) figure), in a table format, thus the table's header row (Titles, marked ③ in the [following](#) figure) is identical to what used to be **The Fields' Tabs** .

As mentioned before, the default set of fields may be altered in:

- Content (which fields out of the 63 will be included), and in
- Order (organization) of presentation.

This is done utilizing the Authority Inspector **Main Menu's File** option and **Initial Authority Collection fields and order** link.

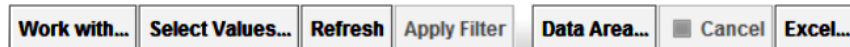
See details in section The Main Menu – File Sub-Menu.



**NOTE:** The **Data Pane** has no influence on the **Filter Pane** of Authority Inspector.

## The Analysis Toolbar

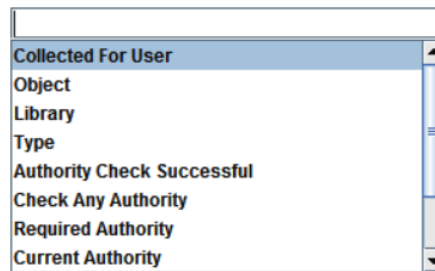
The **Analysis Toolbar** of Authority Inspector is built for auxiliary tasks on the data presented, similar (but different functions) to the Visualizer Analysis Toolbar.



These tasks (presented by activation buttons of the toolbar) are:

### Work with...

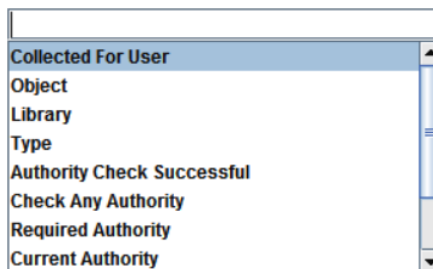
*Button* – Select one out of a pre-defined fields' set for analysis.  
A mouse-click on this button will open the following List Box:



The list includes names of pre-defined fields' collection for Authority Inspector to analyze with.

Selecting the required field is done by mouse clicking on the name, which is similarly achieved by clicking on the **Field' Tabs**.

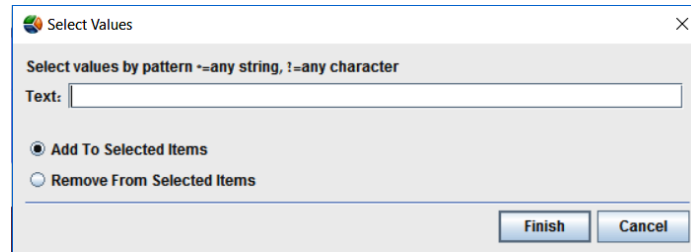
Once a required field is selected, the Authority Inspector **Results Pane** updates immediately to reflect analysis data related to that field.



### Select Values...

*Button* – Enables manual inclusion/subtraction of results' values within the **Tabular Results Presentation Pane**, by name (pattern values allowed) to be added or removed from the filter definition.

A mouse-click on the **Select Values Button** will trigger the following dialog box:



The **Select Values Button** affects the results' set presented in the **Results Pane**.

Names of fields need to be typed-in in the **Text Bar**. These names need not to be accurately spelled since pattern values (use of **\*** and **?** for self-completion) are allowed.

Once all names are typed-in, there is a need to select if these are to be added or removed from the filter definition by marking one of the two (2) Option Buttons provided for this purpose.

Once all the above is set, click with the mouse on the **Finish Button** to set up the filter or the **Cancel Button** to skip the **Select Value** task.

### Refresh

*Button* – If a change was made to the filter's definition by:

- The **Select Values** button or selection of field(s) by mouse clicks on the fields in the **Results Pane**, or
- If new records were added to the analyzed file (the analyzed file might be modified),

Clicking with the mouse on the **Refresh Button** will prompt Authority Inspector to re-examine the server's original Authority Collection database without breaking away from the displayed screen.

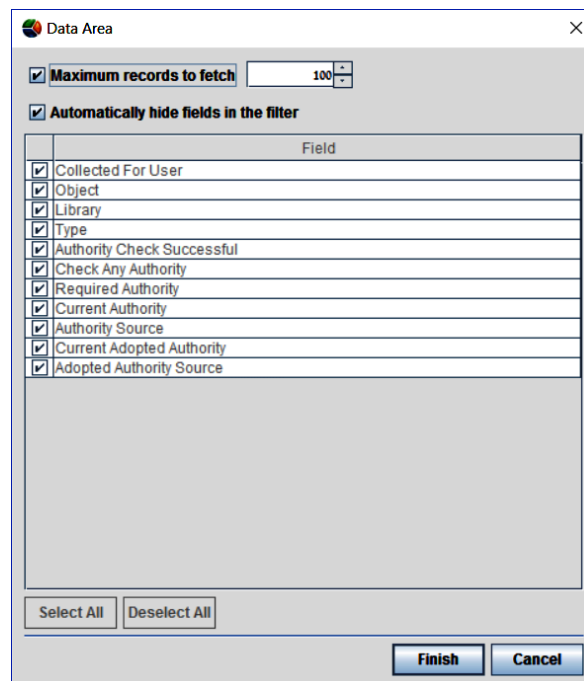
### Apply Filter

*Button* – Unlike Visualizer where this button generated a local operation mainly affecting the graphical results, the **Apply Filter Button** in Authority Inspector generates re-reading operation, from the server's original Authority Collection database, of the data presented in the **Data Pane** to refresh the analysis results and update the display accordingly

### Data Area...

*Button* – The **Data Area Button** resembles, functionality-wise, The Main Menu – File Sub-Menu's option but applicable only to the session in progress (does not set its entered values as defaults).

Once the **Data Area Button** is clicked upon, it will trigger the **Data Area Combo Box** (see figure ) where the **Data Fields** included in the **Data Pane** are listed and may be selected or deselected from the analysis process by check-marking the related Check Box of each one of them.



There is also a possibility to select or deselect all of the fields by clicking on the corresponding buttons.

The **Data Area Combo Box** also enables:

- Setting the number of records to be fetched for analysis by check-marking the box on the top row and setting the number with the counter box.
- Hiding the fields marked from being displayed in the **Data Pane** by check-marking the box on the second row.



*Button* – Operations enabled by the **Analysis Toolbar** may be slowed down if they need to fetch large amounts of data for analysis.

The **Cancel Button** was added for the purpose of canceling such time consuming operations.

**NOTE:** The **Cancel Button** is active only while the red dot is blinking.



*Button* – Similar to the **Excel Button** in Visualizer (see page56), mouse clicking on this button exports the data to an Excel file.

The data exported out of Authority Inspector is:

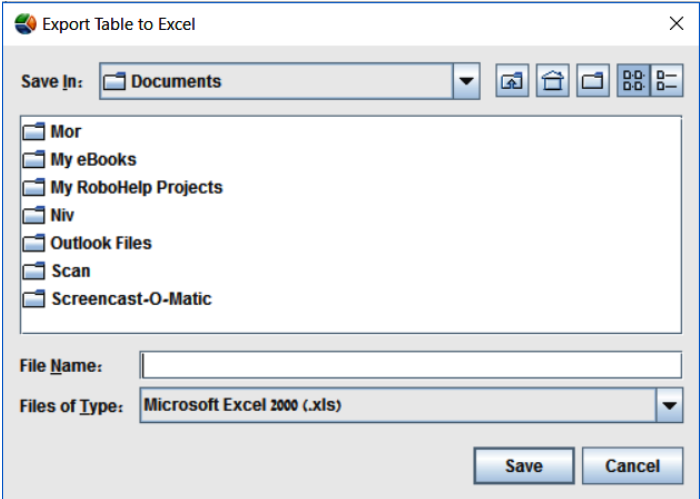
- The data included (and visible) in the **Data Pane** (and not the **Tabular Results Presentation Pane** as in Visualizer), and,
- Only the visible data (e.g. if data was not included due to deselecting It utilizing the above mentioned **Data Area Combo Box**, it will also not be included in the data exported).

Same as in Visualizer, clicking on the **Excel Button** will bring up the **Export Table to Excel Dialog Box** where the resulting Excel file name and storage location need to be set.

Select the storage path for the file and the file name, and then click on



the Save Button



## The Status Bar

The **Status Bar** of the Authority Inspector GUI is also slightly different – two more fields were added:

---

Field: Collected For User | Items Selected: Total: 6-5 | Records Selected: Total: 6-1007 | Data Table: 100 records

- The number of records analyzed (and presented in the **Data Pane**) is displayed on the right side of the **Status Bar**.
- The name of the **Field to Work with** is displayed on the left side of the **Status Bar**.

## Mapping of Field's Content

Some of the Authority Collection fields' data were mapped in the Authority Inspector **Data Pane** display to ease the understanding of their meaning.

These are detailed in the table below:

Field Name	Original Content	Mapped Content
Adopt Authority Used	0	No
	1	Yes
Multiple Groups Used	0	No/Single GrpPrf
	1	Multiple GrpPrf
Authority Check Successful	0	No
	1	Yes
Check Any Authority	0	Specific
	1	Any

# Chapter 5 Configuring the Authority Inspector

---

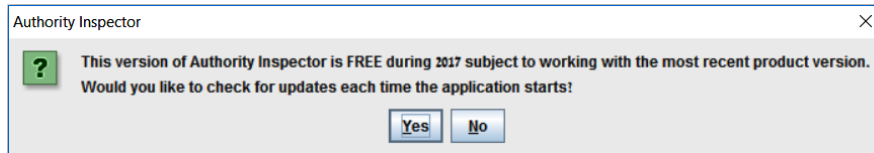
This chapter deals with the configuration (setup) cases of Authority Inspector:

- First-time launching
- Other configuration aspects

# First-Time Launching of Authority Inspector

**NOTE:** Refer to the The Launching Screen paragraph (page 86) for regular everyday launching of Authority Inspector.

Authority Inspector is a product, provided free of charge for evaluation purposes, subject to its being updated when product versions are released. As such, the following Confirmation Box will appear when Authority Inspector is invoked for the first time:



**WARNING:** This **Confirmation Box** will appear only once, upon first activation of Authority Inspector!

Clicking on the **Yes Button** will set the program to automatically check for new versions every time Authority Inspector is invoked.

If Authority Inspector is installed on an off-line PC or if there is reluctance to use such auto-update procedure (mouse-click on the **No Button**), there are two (2) other options to keep Authority Inspector updated:

- From the **Main Menu's Help Sub-Menu** there is a **Check for Update** option to click upon for manual update or
- At the end of every calendar month a message will pop-up to remind the user to manually check for an updated version.

# Configuring the Authority Inspector

---

## The Main Menu

At the top-left side of the Authority Inspector screen there is a **Main Menu** controlling general configuration aspects of Authority Inspector.



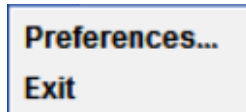
The image shows a horizontal menu bar with a light gray background and a thin black border. It contains two items: 'File' and 'Help', both in a dark gray, sans-serif font.

It includes two (2) Items:

- The **File Sub-Menu**, and
- The **Help Sub-Menu**

## The Main Menu – File Sub-Menu

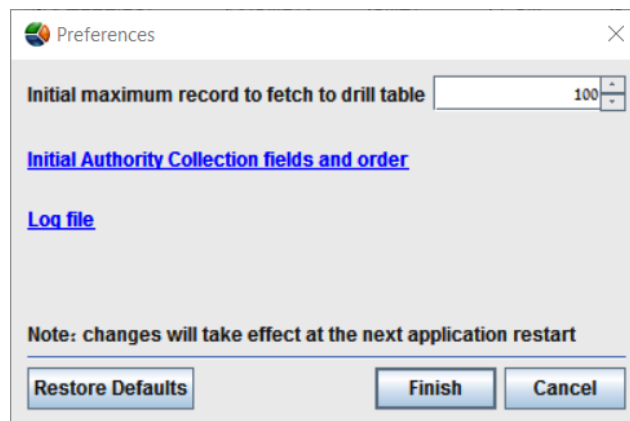
The **File Sub-Menu** includes two options, **Preferences** and **Exit**:



The **Preferences** menu option sets up:

- a. The initial Authority Collection fields and their display order,
- b. The **Log File**,
- c. The maximum number of records to be fetched from the server for processing.

Clicking on the **Preferences** menu option pops up the following Combo Box:



Its functions are:

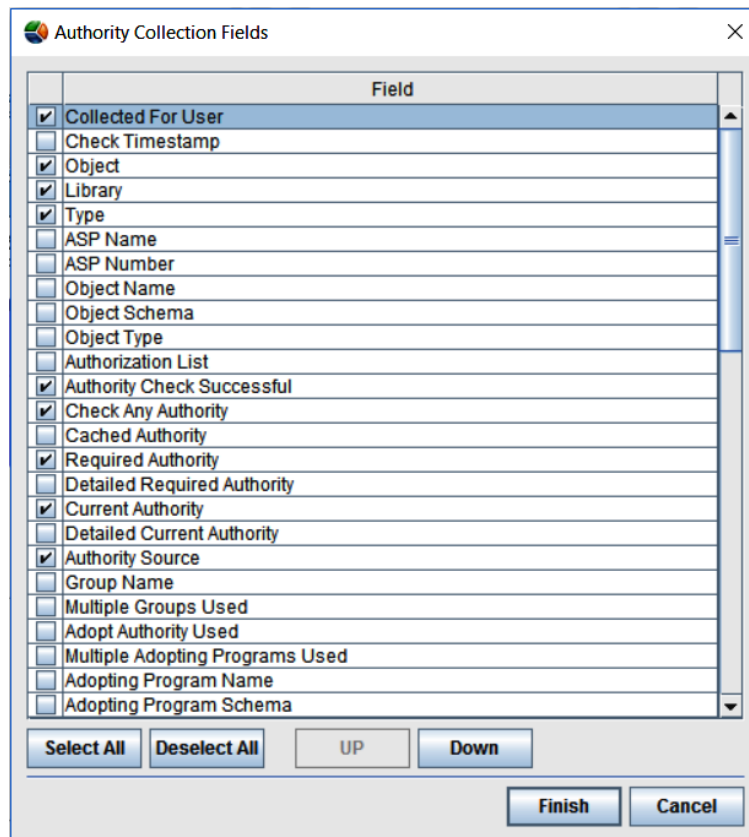
- **Initial Maximum Records to Fetch to Drill Table Spin Box** – for setting the maximum number of records fetched from the server for analysis processing by Authority Inspector.
- **Initial Authority Inspector fields and Order Link** – leading towards another Combo Box (see figure ) enabling the selection of which of the Authority Collection's fields will participate in the Authority Inspector analysis process, and in what order.

Selection is done by marking the check-boxes on the left.



There is also a possibility for **Select All** and **Deselect All** by mouse clicking on the relevant buttons.

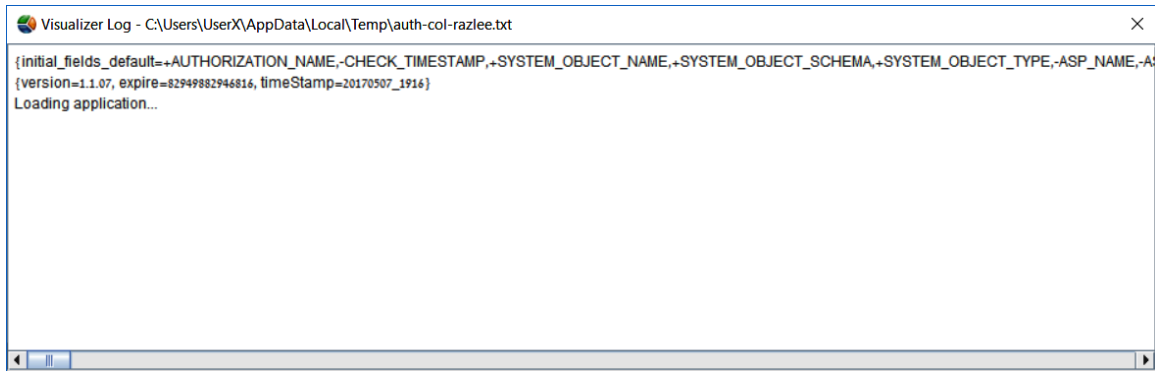
Order is set by highlighting the **Field** with a mouse-click and moving it **Up** or **Down** by clicking with the mouse on the relevant **Up** or **Down** buttons.



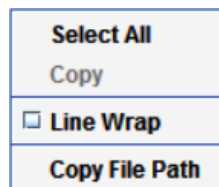
Once the list of participating fields is set, click with the mouse on the **Finish Button** to save it, or the **Cancel Button** to terminate this operation without changes.

- **Log File Link** – Authority Inspector builds, in real time, a log of its operations, mainly for debugging purposes.

Clicking on the **Log File Link** will open the log file as follows:



Right-clicking with the mouse on the log area will open the following Roll-Down Menu:



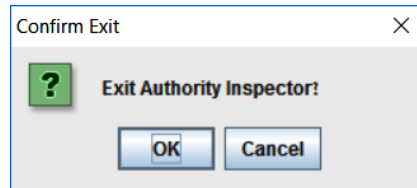
This menu enables:

- **Select All** – Selection of ALL texts included in the log file,
- **Copy** – This menu-option allows copying of the entire text (in case **Select All** was marked) or partially selected and marked texts (using the mouse and the keyboard's **C** button) for reporting purposes,
- **Line Wrap Check Box** – Wraps the text within the display window (the above screen capture of the Log File is presented unwrapped),
- **Copy File Path** – Also for reporting purposes, this menu option allows copying of the Log File's path.
- **Restore Defaults Button** – Mouse clicking on this button restores all default values of Authority Inspector.

Once all configurations are set, there is a need to mouse click on the **Finish Button** to store them.

In case of an error – click on the **Cancel Button** and all changes will be ignored.

The **Exit** button closes the Authority Inspector program.

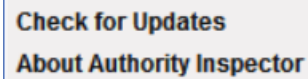


Clicking on the **Exit Menu Option** will pop-up the **Confirm Exit Message Box** where clicking on the **OK Button** authorizes the exit and shuts-off the Authority Inspector program.

Clicking on the **Cancel Button** cancels the exit operation.

## The Main Menu – Help Sub-Menu

The **Help Sub-Menu** includes two (2) options:



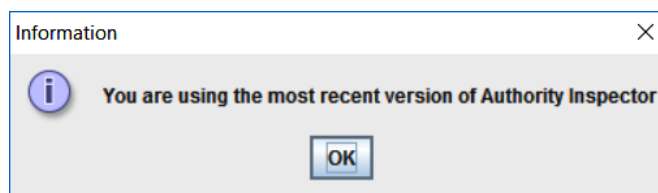
Check for Updates  
About Authority Inspector

- **Check for Updates** – This menu option was mentioned in the First-Time Launching of Authority Inspector section (page 101).

**NOTE:** Usage of this menu option requires access to the internet.

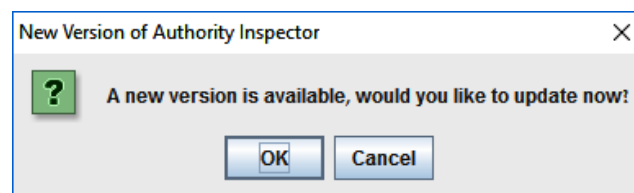
Once activated with a mouse click, Authority Inspector will check for the availability of a new version.

If the current version was found to be the most update one, it will generate the following Message Box:

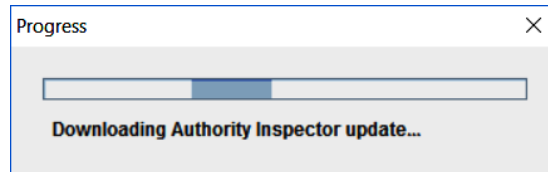


Click on the **OK Button** to release the Message Box.

If a new software version was found, the following Message Box will pop-up:



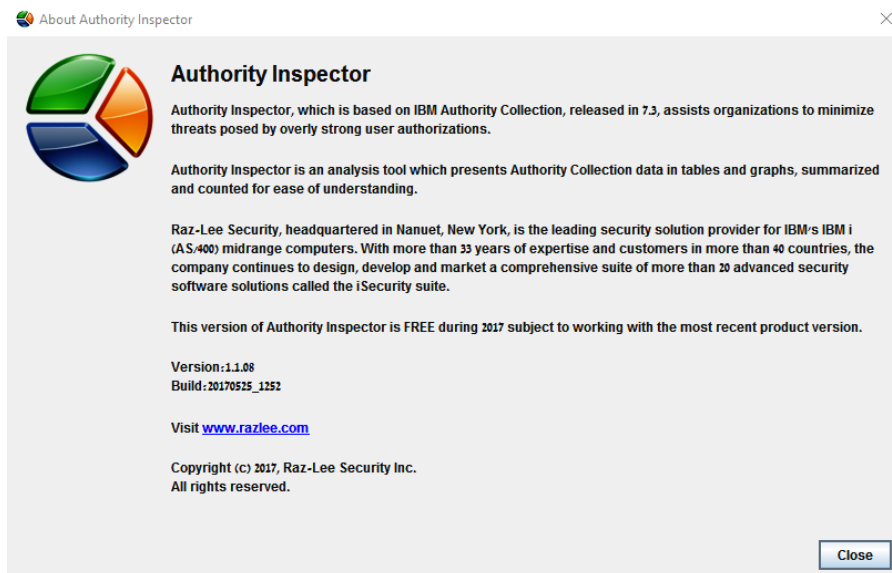
Clicking on the **OK Button** will trigger downloading of the new version onto the PC, supplemented with the following Progress Meter:



Upon completion of the download, the new version will be automatically installed and launched.

- **About Authority Inspector** – This menu option provides general information about the currently installed software.

Clicking on this menu-option will pop-up the following Message Box:



Click on the **Close Button** to release this Message Box.

## Chapter 6 Using the Authority Inspector

---

The basic concept of analyzing Authority Collection security related activities is by creating progressive approximating filters (queries), one step at a time, to filter the specific event(s) searched for and all system data related to these event(s).

Let us take a security threats related example based on Authority Inspector.

The scenario we examine is:

*A credit-card firm decides to explore its IBM i objects for vulnerability caused by excessive authorities which exposes the security level of its credit-cards' data to hacking risks.*

*Known facts which supports such an examination, are:*

- *The library names of libraries storing the data are all starting with SMZ,*
- *The data included in IBM's Authority Collection **Current Authorities** and **Required Authorities** fields is not detailed enough for this task.*

*To expose these vulnerable objects there is a need to compare Current Authorities with the Required Authorities.*

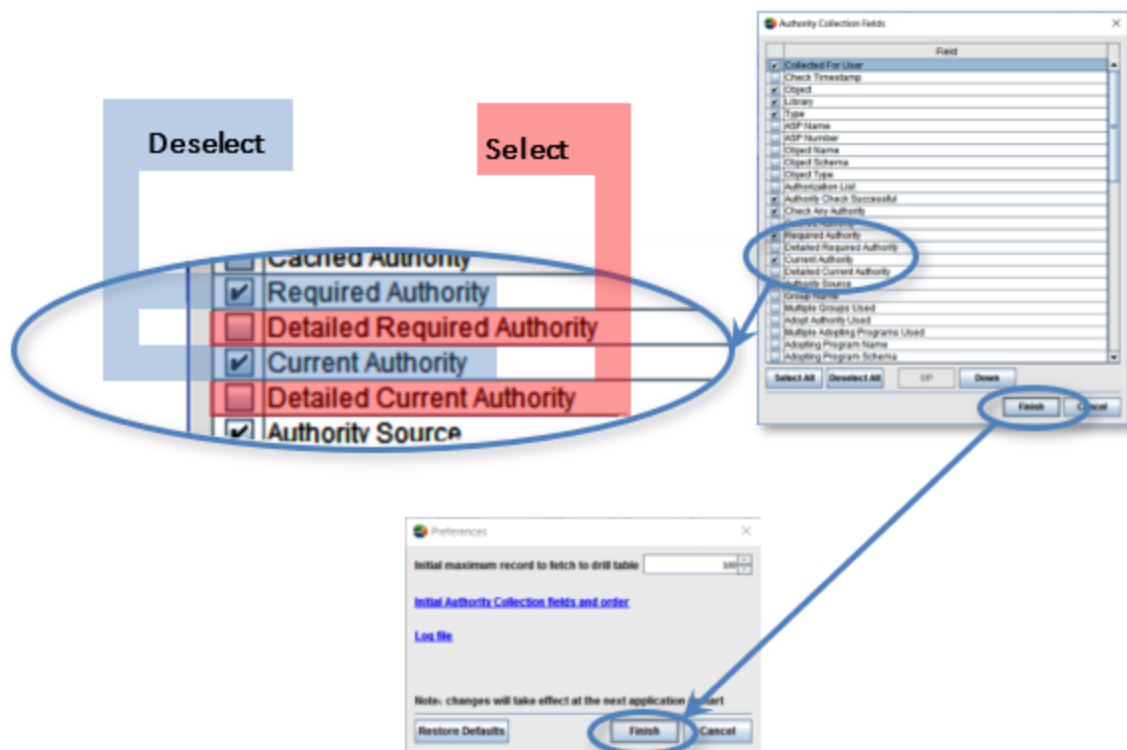
## Setting up the Filters

Since the data included in the IBM i Authority Collection's **Current Authorities** and **Required Authorities** fields is not sufficient for this task while these fields were included in the default field-set of Authority Inspector, there is a preliminary requirement to replace them with the more detailed fields – **Detailed Current Authorities** and **Detailed Required Authorities**.

This is done by utilizing the **Main Menu's File > Preferences > Initial Authority Collection fields and order** as demonstrated in the figure Setting up the Filters.

The **Current Authorities** and **Required Authorities** fields may be deselected and the **Detailed Current Authorities** and **Detailed Required Authorities** fields should to be selected.

Then, the **Finish Button** need to be mouse clicked upon and clicked upon again in the **Preferences Combo Box** to complete the fields' replacement.



**NOTE:** Following the above, Authority Inspector must to be terminated (**Main Menu > File > Exit**) and re-started to save the change.

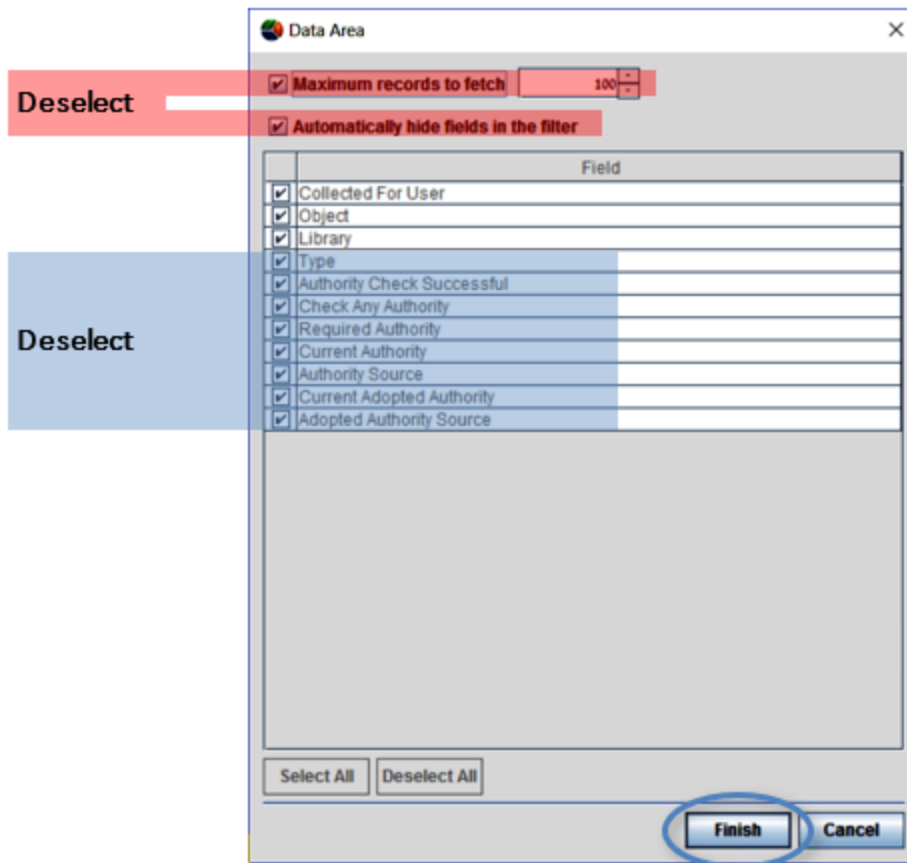
For the next drill-in step, click on the **Data Area Button** in the **Analysis Toolbar** to open the **Data Area Combo Box** where:

1. The **Maximum records to fetch** and the **Automatically hide fields in the filter** options might be deselected for our purpose.
2. The fields not required for the analysis need to be deselected as well.

As demonstrated in the figure .

The above steps ensure that only the data required for the analysis process will remain.

The remaining **Object**, **Library** and **Type** fields are unique identifiers of any object in the IBM i system and **MUST** be included in such an analysis if searching for object authorities.



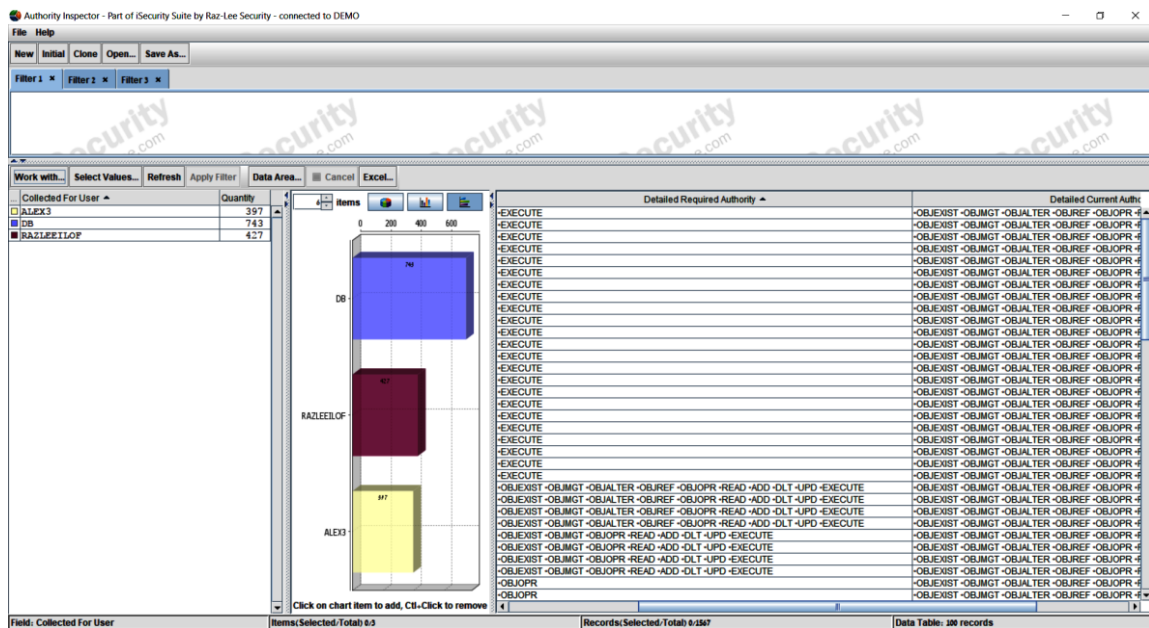
The **Results Pane**, including the **Tabular Results Presentation Pane**, the **Graphical Results Presentation Pane** and the **Data Pane**, are immediately updated according to the above filter definitions, as demonstrated in the figure below.



**NOTE:** Each row of the **Data Pane** table represents a single object.

Even at this early step of the process, there is an already obvious general view of where the problem lays – comparison of the objects (the table rows) in the **Detailed Current Authorities** and **Detailed Required Authorities** columns (highlighted in the figure above with semi-transparent red and blue) in the **Data Pane** visually stand-out to reveal the fact that there are far more Current Authorities than Required Authorities.

This means – there is certainly an inherited vulnerability problem caused by excessive authorities which jeopardizes the security level of the credit-cards' data, since the system acquired more authorities than planned for by the programmer (or the system administrator).



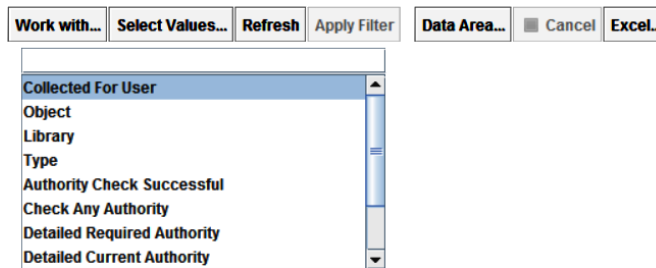
The **User Profile** that interacted with each object can be seen in the **Collected for User** column allowing initial identification of where the problem might be.

Therefore it would be practical to filter them out for close examination of where the problems may be found.

For that purpose the screening process may begin by screening the objects included only in the libraries storing the data of interest (all libraries with names starting with SMZ, see Known facts which supports such an examination, are:).

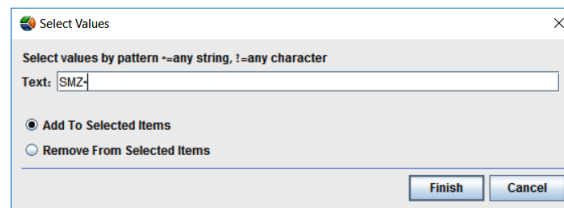
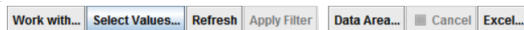
The steps to screen these objects are:

1. Mouse click on the **Work with Button** of the **Analysis Toolbar** and click on the **Library** option in the Drop-Down Menu that opens to select the **Libraries** as the pivot for filtering the data, as demonstrated in the figure below.



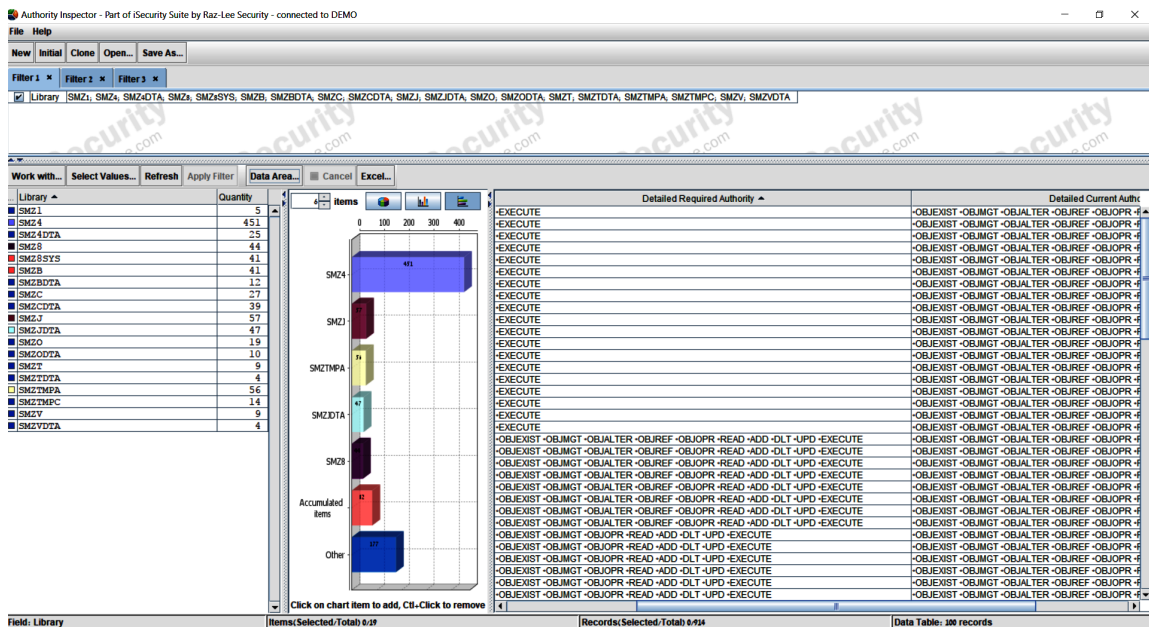
2. Mouse click on the **Select Values Button** (of the **Analysis Toolbar**) and in the **Select Values Combo Box** that opens, type-in – SMZ\* (not case sensitive). This means – all libraries with names starting with SMZ.

To conclude this step, mouse click on the **Finish Button** to end the library selection and save its results.



3. Mouse click on the **Refresh Button** and the screen will update accordingly:
  - The **Tabular Results Presentation Pane** include only the SMZ\* objects,

- The **Graphic Results Presentation Pane** and the **Data Pane** presents the analysis results accordingly.



4. Further investigation could be made by limiting the analysis results to include only programs and commands.

This is done by mouse clicking on the **Work with Button** of the **Analysis Toolbar**, selecting the **Type** option, and highlighting **\*PGM** and **\*CMD** fields.

Clicking on the **Apply Filter Button** in the **Analysis Toolbar** will update the screen to show the new filtering results (watch the **Filter Definition Pane**, the **Tabular Results Presentation Pane**, the **Graphic Results Presentation Pane** and the **Data Pane**).

Mouse clicking on the **Detailed Required Authorities column** in the **Data Pane** will re-arrange the table and make it clear to the investigator that many objects which originally had **\*EXECUTE** authority only inherited many other (probably jeopardizing the security level of the) data.

5. Further investigations are possible too, for example – filtering some specific users or objects, until the investigator narrows down the possible jeopardizing objects.

**NOTE:** To investigate the source for these inherited excessive authorities please use other Raz-Lee software products such as Audit.

