RAZ-LEE

iSecurity GUI

User Guide
Version 5.0

www.razlee.com

Contents

–

-

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 GUIUser 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.

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 page 6.

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

COMMAND > 81 > 32

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

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

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

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

Introducing iSecurity

What is iSecurity?

iSecurity is a comprehensive network security solution that completely secures your System i against all known external threats, and also controls what users are allowed to do **after** access is granted. iSecurity is a robust, cost-effective, security solution.

iSecurity is by far the most intuitive and easy-to-use security software product on the market today. Its top-down functional design and intuitive logic create a work environment that even novices can master in minutes. iSecurity features a user-friendly, Java-based GUI and an System i Navigator (OpsNav) plug-in.

Why You Need iSecurity

When it was first launched, the System i was used almost exclusively in a closed environment, with host systems connected to remote data terminals via proprietary technologies. Within this closed environment, the security features of the IBM i (OS/400) operating system provided the strongest data and system security in the world. User profiles, menus, and object level security provided all the tools necessary to control what users were allowed to see and do.

In today's world of enterprise networks, PCs, distributed databases, the Internet and web technologies, closed computing environments are all but extinct. Technological advances compelled IBM to open up the System i and its IBM i operating system to the rest of the world. This new openness brought with it many of the security risks inherent in distributed environments.

The simple fact is that users accessing the System i and its databases externally can easily bypass native IBM i security. System administrators need to equip themselves with a new generation of security tools to combat these evolving threats. iSecurity is just such a tool. It enhances native IBM i by controlling access via all known external sources and controlling precisely what users are permitted to do after access is granted.

How iSecurity Works

Top-Down Security Design

Top-down security design means that the process of designing and applying security rules follows the most efficient and logical path possible. In other words, this means you have to design far fewer rules in order to achieve maximum security and your System i needs to process apply rules to far fewer transactions than many similar products. You save planning and maintenance time, and also valuable system resources.

Top-down security designs a simple hierarchy of rule types. When a higher level rule type fully meets your security requirements, you do not need to define any more rules for that situation. The following drawing illustrates this concept.
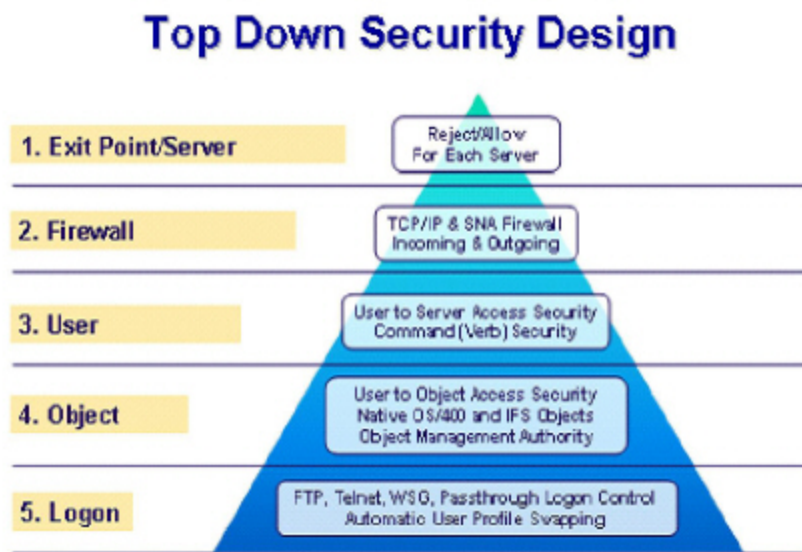
System i security is based on five basic levels:

- Server/Exit Point Security
- TCP/IP Address Firewall Security
- User-to-Service Security
- Object Security
- Logon Security (provides additional security features after access has been granted)

Simply put, whenever a higher, less specific rule will suffice, you do not need any more specific rules. For example, if you do not need to use FTP, you simply reject all transactions at the FTP Server/Exit Point level. You do not need to define any rules that limit FTP access via specific IP addresses, by specific users, or to specific objects.

iSecurity Rules and the Best Fit Algorithm

iSecurity is a rules-based security product. You create a wide variety of rules to cover many different situations and to counter different kinds of threats. Some rules will likely apply globally to all or most activity types while others will be designed to cover very specific situations.

You can enable FYI Simulation mode globally for all activity regardless of server or user. You can also enable FYI individually for specific function servers as a parameter in server security rules. In this manner, you can test security rules for specific servers without affecting rules that apply to other servers.

FYI Simulation Mode

FYI Simulation mode allows you to simulate the application of security rules without physically rejecting any activity. All rejected transactions are recorded in the Activity log as such, but the activity is allowed to proceed without interruption. This feature allows you to test your rules under actual working conditions without adversely affecting user success.

FYI Simulation mode may be enabled globally for all activity or enabled for individual function servers. In this manner, you can test security rules for specific servers without affecting rules that apply to other servers.

Emergency Override

The Emergency Override feature allows you to override all existing security rules temporarily by allowing or rejecting all activity. This feature is useful to respond quickly to emergencies such as critical transactions being rejected due to problems with iSecurity security rules or a sudden security breach.

Rule Wizards

The unique Rule Wizards feature makes security rule definition a snap, even for non-technical system administrators. This user-friendly feature allows you to view historical activity together with the security rule currently in effect on a single screen. You can even modify the existing rule or define a new rule without leaving the wizard. The Rule Wizards are an invaluable tool for defining the initial set of rules after installing iSecurity for the first time.

Activity Log

The Activity Log provides complete details of every transaction captured by a security rule. You have full control over which activities are included in the Activity Log and under which conditions.

Highly-defined filter criteria allow you to select only those records that you need to examine by using Boolean operators and the ability to combine complex logical conditions. You have full flexibility to specify the sort order according to multiple fields.

Visualizer BI

Visualizer BI is an advanced data warehouse solution for graphically displaying security data. It allows IT managers to analyze security-related system activity quickly and easily using a graphical interface. Visualizer BI eliminates the need for time-consuming log-scanning and tracking activities that tie up system resources and increase operating costs.

System Requirements

- PC workstation - (due to the use of Java 6)
  - Windows XP Professional (SP1)
  - Windows XP Home
  - Windows 2000 Professional (SP3+)
  - Windows Server 2003, Web Edition
  - Windows Server 2003, Standard Edition
  - Windows Vista
  - Windows 7
  - Windows 8
  - Windows 10
- Operating system: GUI connects to V5R3 and higher of IBM i (OS/400)
- Minimum RAM: 128MB
- TCP/IP communication to the System i (AS/400).
- STRTCPSVR SERVER(*DDM) to start the TCP/IP server (with *DDM specified for the Server parameter).
- Host servers should be started on the server. (STRHOSTSVR SERVER (*ALL)) from the System i (AS/400) command prompt).
- QUSER user profile enabled and with a valid password.
- Disk space required: 160MB

Getting Started

Overview

This chapter describes the working environment of the iSecurity GUI, including its various panels, screens, menu bars, tool-bars, and icons. In addition, it describes how to set up accounts, connect to sessions, and configure the GUI.

Although throughout this manual there is a top level discussion of working with the unique features of the GUI, there is no description of how to perform functions that are also available on the native version of the system. These functions are duplicated here, and for an explanation of how to fill in the various forms and fields, you should consult the appropriate product manual.

Creating a New Account

1. Double-click the iSecurity icon on your desktop.
2. Right-click in the iSecurity navigator view.
3. Select **New Account...** The **Account Name** panel in the **New Account** dialog is displayed.
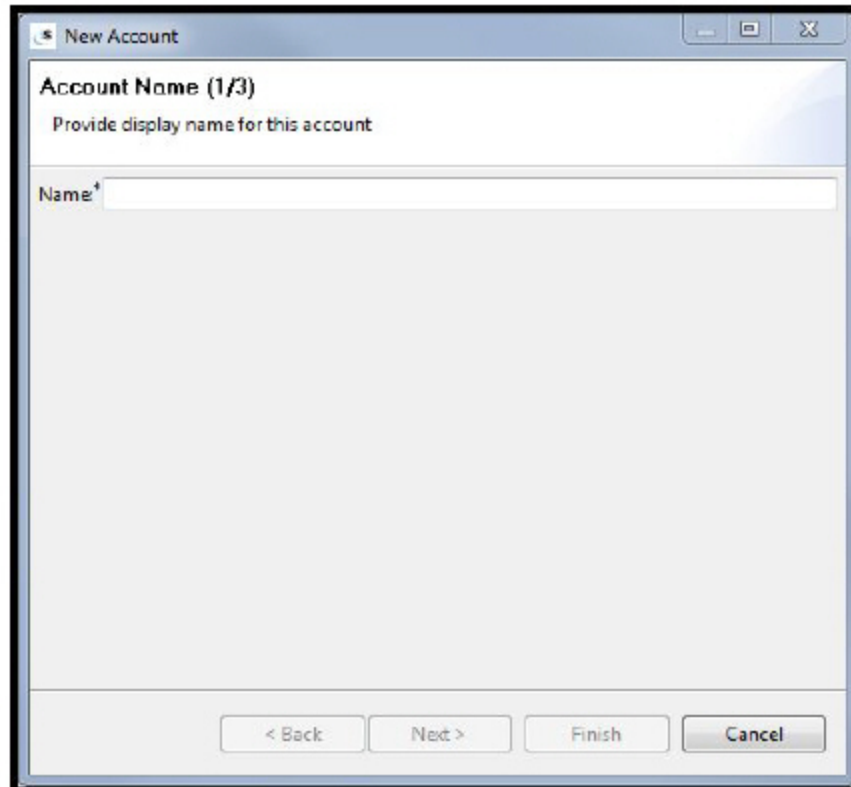
4. Enter the account name and click **Next**. The **Connection** panel in the **New Account** dialog is displayed.
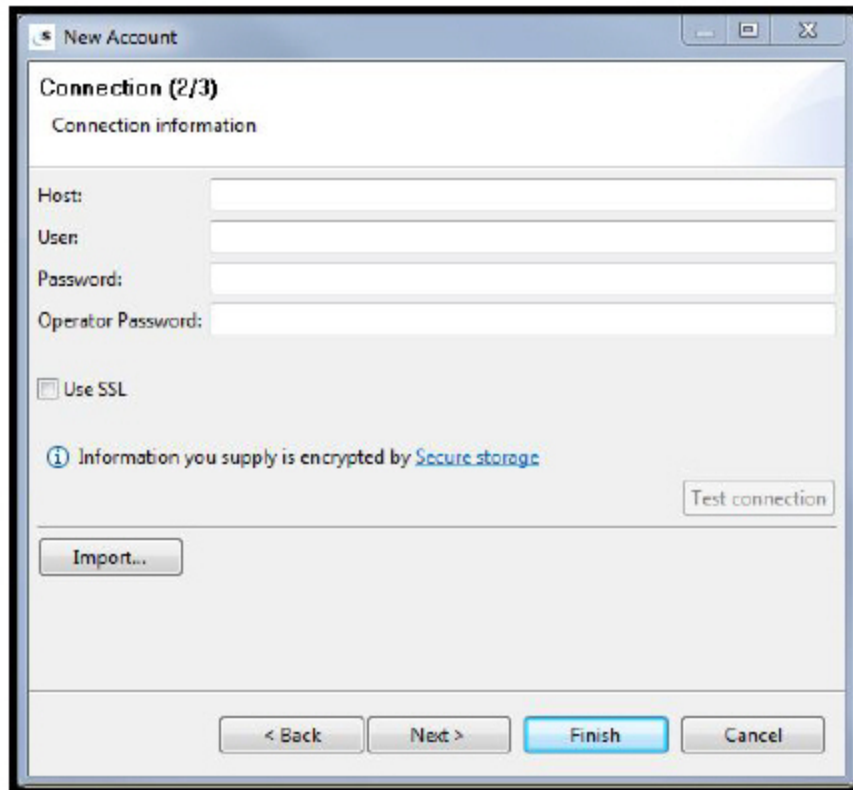
5. In the **Connection** panel, enter **Host**, **User**, and **Password** in the correct fields, and click **Finish** or **Next**.

6. If you clicked **Next,** the **Connection Control** panel in the **New Account** dialog is displayed.
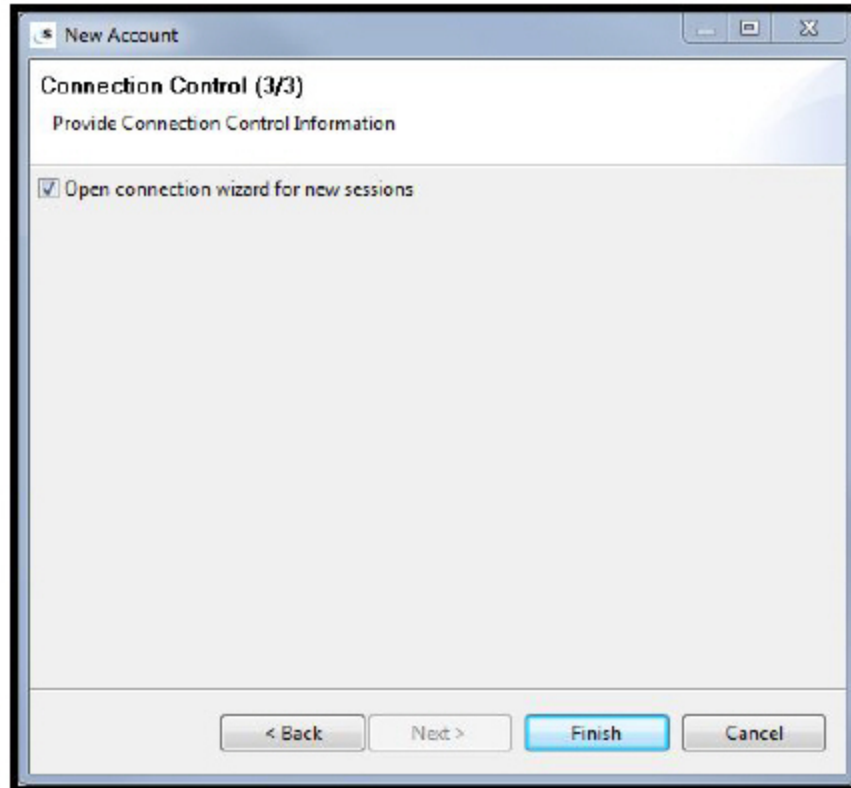
7. Check the **Open Connection Wizard** if you want the application to prompt you for new sessions. This is just a conveniences issue that suits those cases where all required information for making a connection is supplied.

Running iSecurity GUI in SSL mode

Encrypt the link between any sensitive file and the GUI interface using the Eclipse SSL system.

1. Navigate to your **System i** in a web browser, using the address `http://<IP_Address>:<PortNumber>`, where `IP_Address` is the IP address of your System i and `PortNumber` is usually `2001`. You can get both parameter values from your System Administrator. The **iSeries Tasks** screen is displayed.
2. Click **Digital Certificate Manager** from the list of tasks. The **Digital Certificate Manager** screen is displayed.
3. Click **Install Local CA Certificate on Your PC** in the left hand pane.
4. Click **Copy and paste certificate**. The certificate is displayed.
5. Copy and paste the certificate into a text editor, and save the file with a meaningful name such as **ca.txt** to the iSecurity installation directory (the default directory is **C:\Program Files (x86)\iSecurity 4**).
6. On your local computer, open the command prompt and change the directory to the iSecurity installation location (the default location is **C:\Program Files (x86)\iSecurity 4**).
7. From that location, use the Java tool **keytool** to import the certificate into a trust list. Run the following command:
   jre\bin\keytool -import -v -trustcacerts -alias <aliasName> -file ca.txt -keystore trustlist (alias is just optional).
   This will create a file called `trustlist`; while the command is running, you will be prompted to create a password for this file.
8. This step can be performed either from command line or from within the GUI itself.

*Command line: From the command prompt from within the iSecurity installation directory, run this command:

isecurity.exe -vmargs -Djavax.net.ssl.trustStore=trustlist-Djavax.net.ssl.trustStorePassword=pwd

Replace `trustlist` and `password` with your own (these are the parameters used in step 3)

-

The **trustlist** parameter is the absolute path to the file itself including file name (c:\....\trustlist) but if this file resides in the iSecurity installation location, there is no need to type the path.
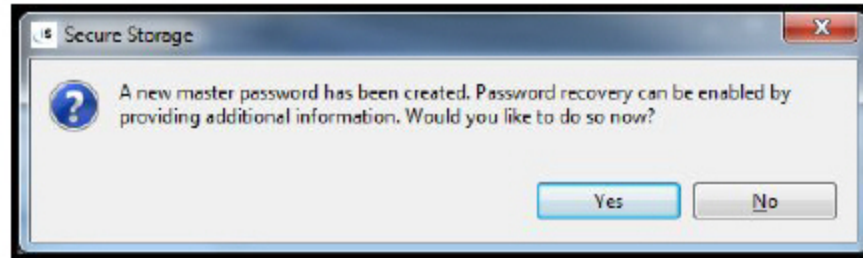
SSL Settings

1. In the menu bar, select **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the left-hand pane, select **SSL Settings**.
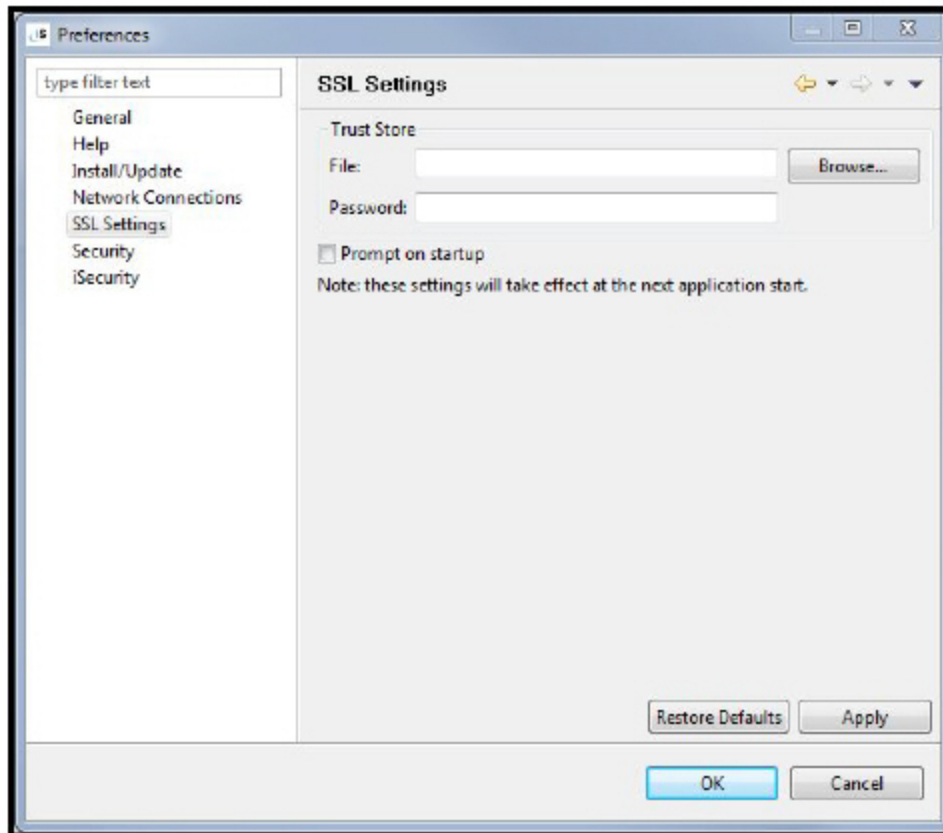
3. To keep the SSL connection in high security level, check the **Prompt on Startup** check box and leave the **File** and **Password** fields empty. If you do not want the prompt, type the file name and access password and leave the check box empty.
4. Click **Apply** or **OK**. These settings take effect only when you next start the application.

    Windows users: a Master Password is automatically created according to the Windows logon user/password in use.

Linux users: the **Create a Master Password** dialog is displayed.

5. Next time the iSecurity GUI starts, the **SSL Settings** dialog is displayed, asking for the secured file name and access password.

Security

Secure Storage

The secure storage definitions are located at: **Window -> Preferences -> Security ->Secure Storage** and saves data in an encrypted form. On some operating systems, it uses your operating system account information to provide a single sign-on experience.

The secure storage also contains the Windows account information in an encrypted form, which means that without the Windows account password there is no access to the System i (AS/400) sensitive data.

NOTE: Read more about Secure Storage in the Eclipse Platform Help.

Set an Alternative Secure Storage Location

There are many reasons to set an alternative secure storage location. For example, your organization's security policies might not allow you to use the default Secure Storage location. You may also want to have an alternative location for fall-back purposes. After you have created the new location, you must update the iSecurity **ini** file and verify access to the system.

1. In an accessible location, create an empty file called **secure_storage**, and save its full access path.
2. Navigate to the **iSecurity.ini** file and open it in any text editor (the default directory is the iSecurity installation directory: **C:\Program Files (x86)\iSecurity 4**).
3. At the end of the file, add the following two lines:

```
-eclipse.keyring
```

<FileLocation>secure_storage

where **<FileLocation>** is the full access path of the **secure_
storage** file you created in [step 1](#).

4. Save and close the file. You can now start the GUI and define accounts.

Run iSecurity With No Permanent Secure Storage Definition

You can run iSecurity without defining the Secure Storage location to the iSecurity system. This procedure assumes that iSecurity is installed in its default location of **C:\Program Files (x86)\iSecurity 4**).

1. In an accessible location, create an empty file called **secure_storage**, and save its full access path.
2. Open a DOS command window and enter the following two commands:

   cd "Program Files (x86)\iSecurity 4"

   iSecurity.exe -eclipse.keyring <FileLocation>secure_storage
   where **<FileLocation>** is the full access path of the **secure_
   storage** file you created in [step 1](#).

Delete Secure Storage

To delete the Secure Storage information:

1. In the menu bar, select **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the left hand pane, select **Security ->Secure Storage**.
3. Select the **Contents** tab.
4. Click to select the **Default Secure Storage**.

-
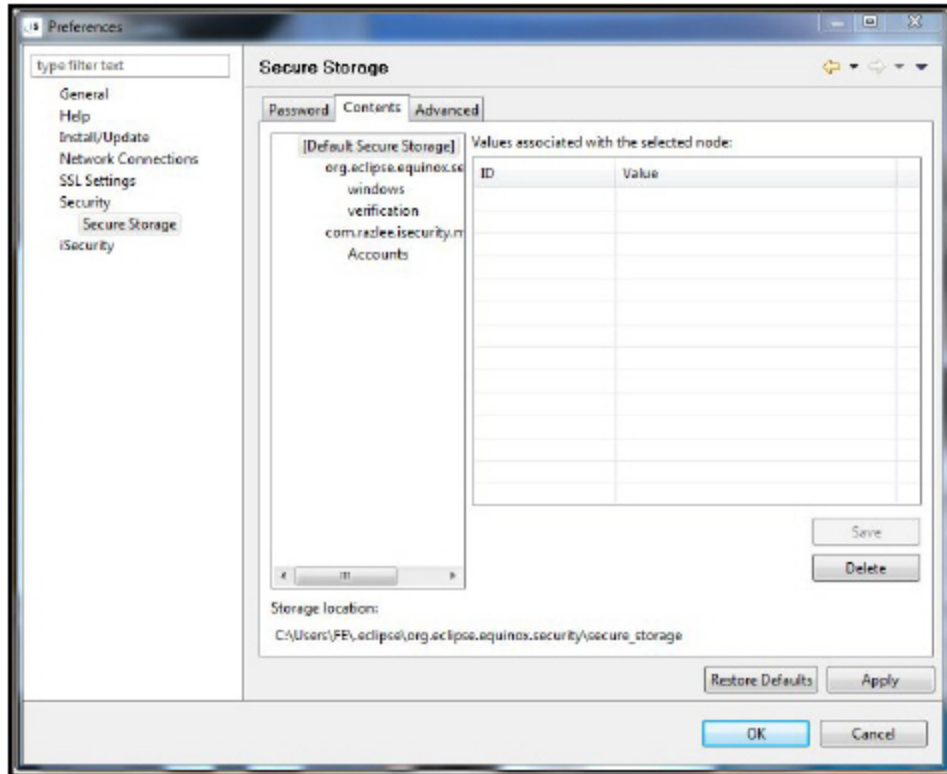
5. Click **Delete** to clear the storage.

Account Information Properties

After you have created the account, it is added to the iSecurity navigator.
You can modify an account by right clicking on it and selecting **Properties**.
The **Properties** dialog is displayed.
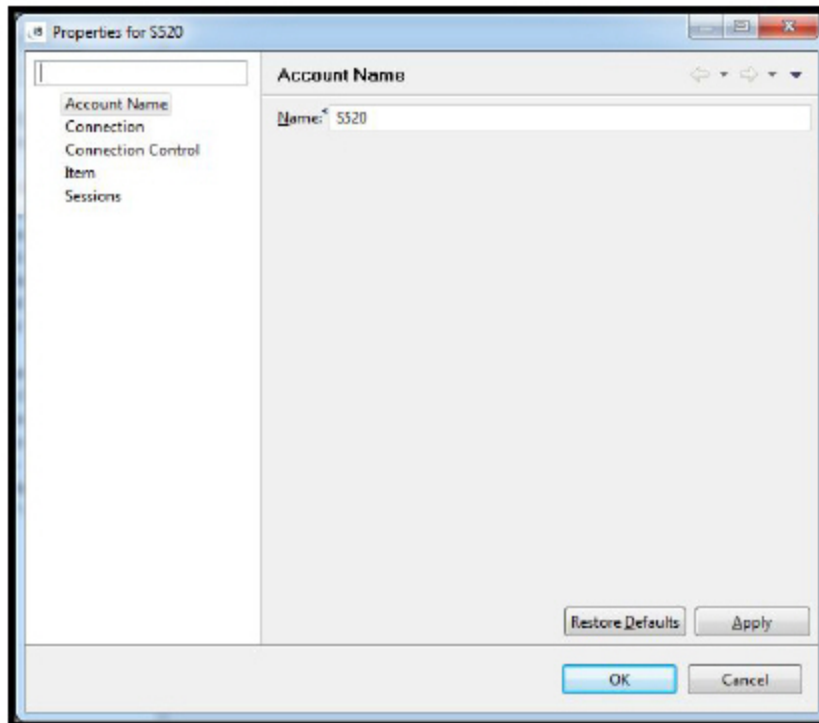
Account Name

Select **Account Name** to change the Account Name.

Connection

Select **Connection** to view the connection details for the account.
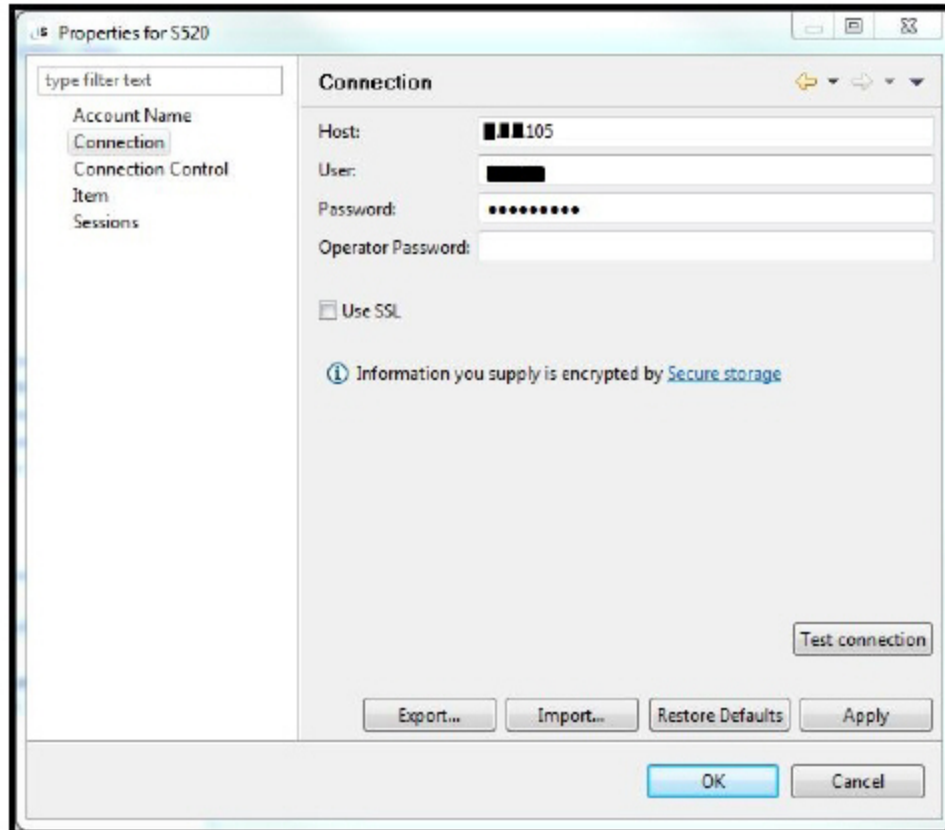
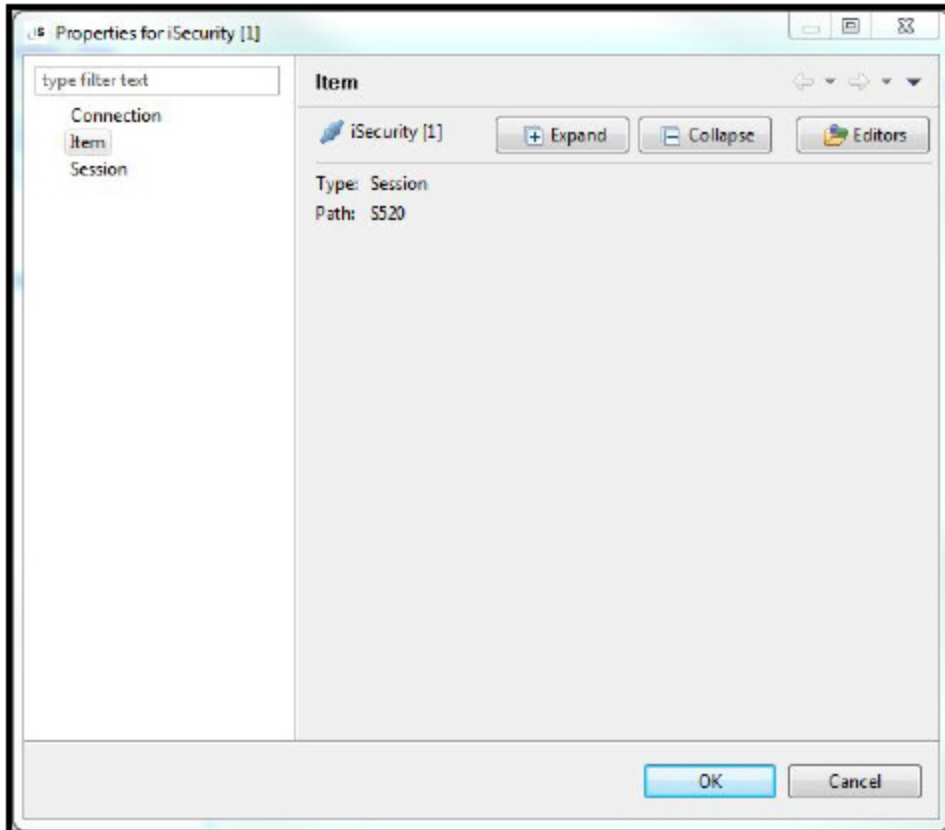You can export the connection details to an XML file, import new connection details from an XML file, or test the connection.

Connection Control

Select **Connection Control** to define how new sessions should be opened for this Account.
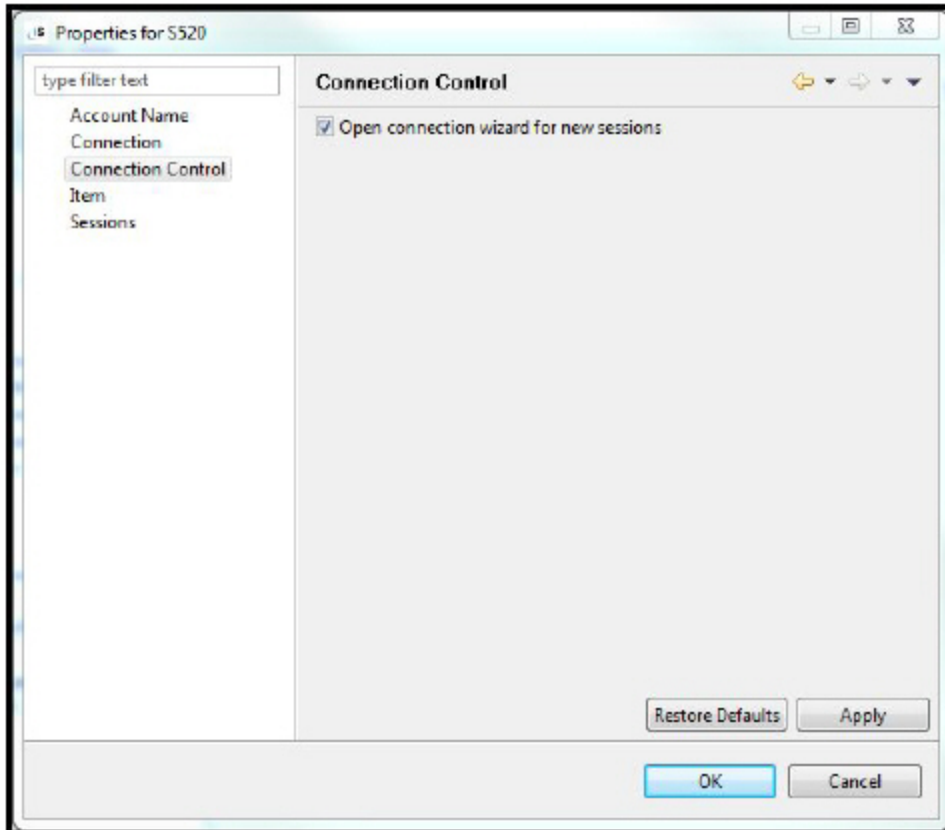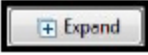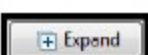
If you select **Open connection wizard for new sessions**, you will be able to enter different Connection parameters for the new sessions. If you clear **Open connection wizard for new sessions**, all new sessions will be opened using the Connection parameters defined for the account.

Item

Select **Item** to control how you view the account in the navigation pane and also to access editors directly without using the navigation pane.

| Option	Description
⊞ Expand	In the navigation pane, opens all the nodes of the Account.
⊟ Collapse	In the navigation pane, closes all the nodes of the Account.
⊞ Expand	Opens the **Editors** dialog, which displays all the available Editors in alphabetical order. This allows you to select an Editor without knowing its location in the navigation pane.

Account Sessions

Select **Sessions** to view how many sessions are open for this account.
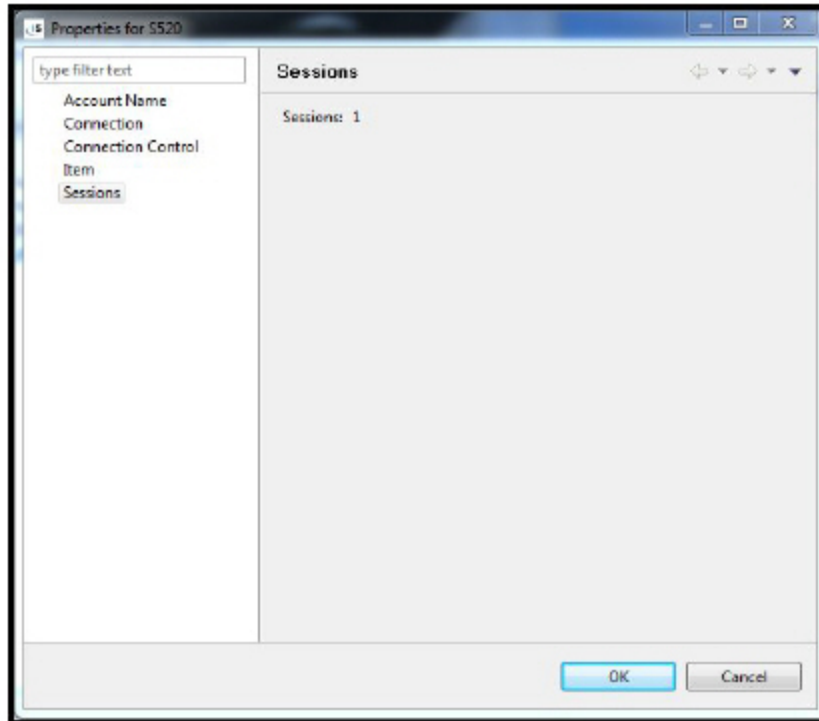
Deleting an Account

To delete an Account, right-click on it and click **Delete**.

Deleting the account will disconnect all sessions for that account.

NOTE: If a session has unsaved data, the user will receive a warning asking for confirmation of the action.

Sessions

Creating New Sessions/Connections

Single and Multiple sessions/connections can be added to one or more accounts.

To create new accounts:

1. Right click the account and select **New Session**.
2. Double click the account (if it has not got sessions).
3. Click on the node's handle (if it has not got sessions)

   NOTE: You can open multiple sessions for one account.

   The **New Session** dialog is displayed.
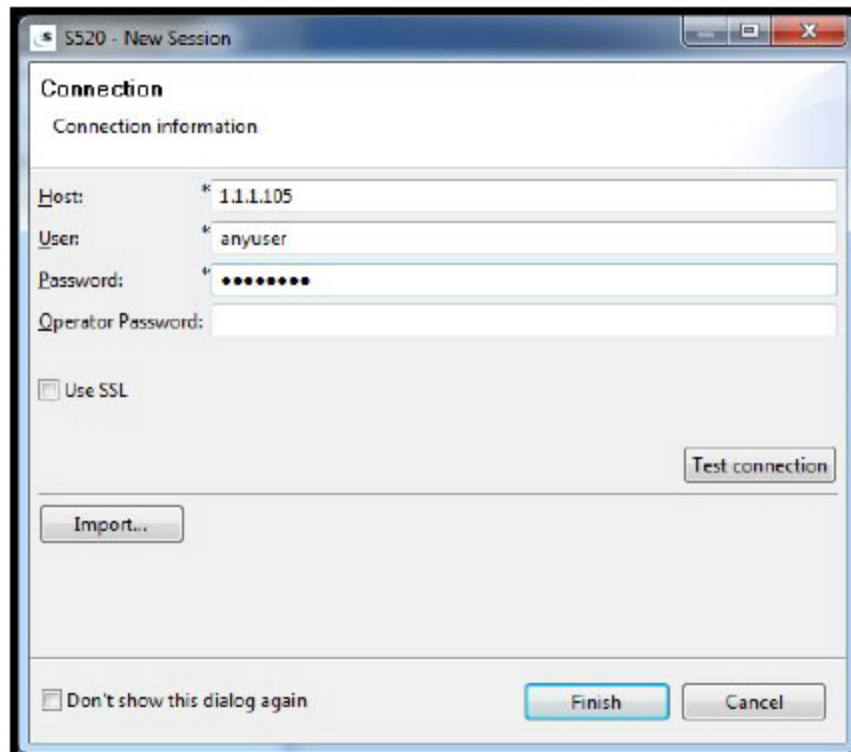
4. Click **Import** to import connection data that was saved on creation of an account.
5. Check the Don't show this dialog again check-box to prevent prompting for new sessions for this account.

   NOTE: Data supply in this step has no persistence on disk.

6. Click **Finish** to connect to the supplied host. The connection process runs in the background, allowing the user to continue working.

A new session node is added to the account along with the nodes of the application.
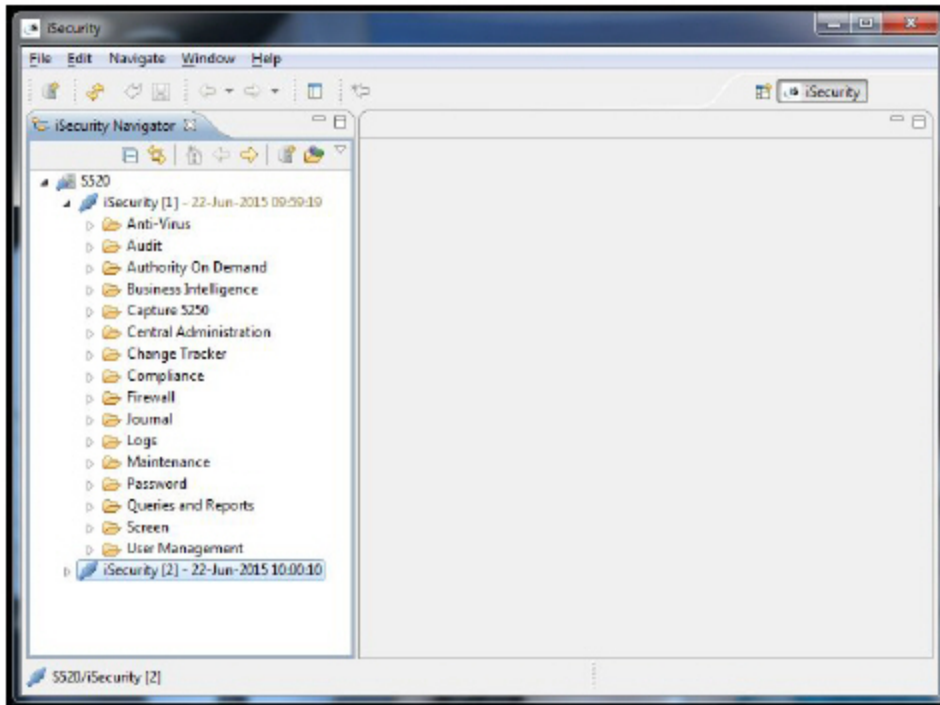
Disconnecting a Session

To disconnect from a session, right click on a session title or on multiple sessions and select **Disconnect**.

Session Properties

You can view the Session properties by right clicking on it and selecting **Properties**. The **Properties** dialog is displayed.

Connection
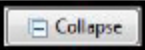
Select **Connection** to view the connection details for the Session.The properties are read-only and cannot be modified.

Item

Select **Item** to control how you view the account in the navigation pane and also to access editors directly without using the navigation pane.

Option	Description
⊞ Expand	In the navigation pane, opens all the nodes of the Session.
⊟ Collapse	In the navigation pane, closes all the nodes of the Session.
⊞ Expand	Opens the **Editors** dialog, which displays all the available Editors in alphabetical order. This allows you to select an Editor without knowing its location in the navigation pane.

Session

Select Session to view information about which products are authorized for the session and which Series i jobs are running under this session.

The **General** tab of the **Session** properties lists the authorization level for each product.
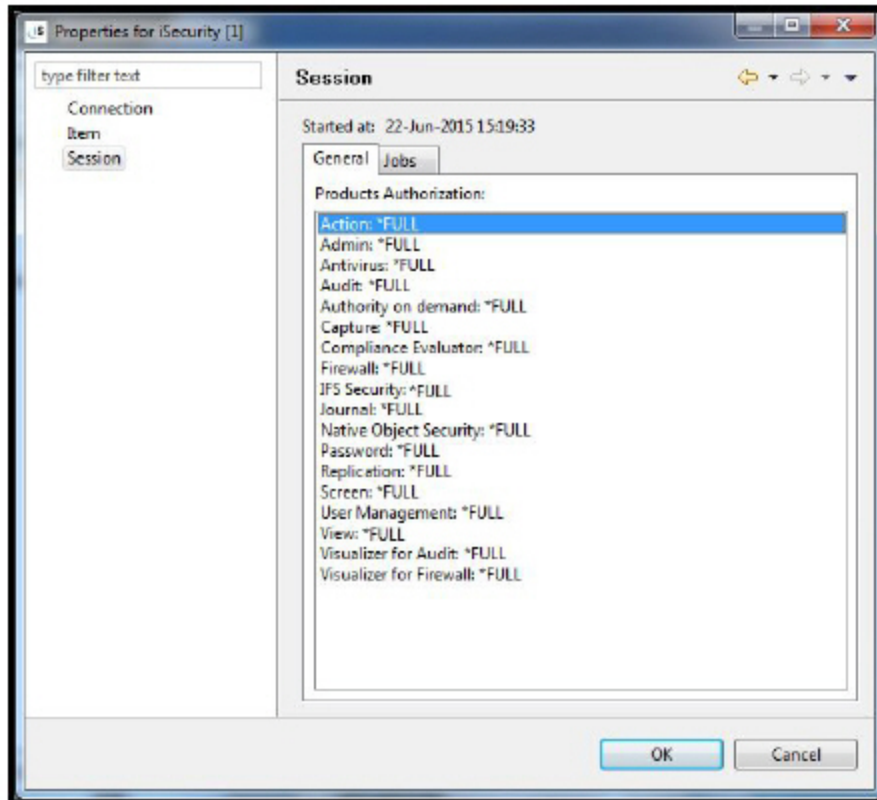
The **Jobs** tab of the **Session** properties lists the IBM i (AS/400) jobs running for the session.
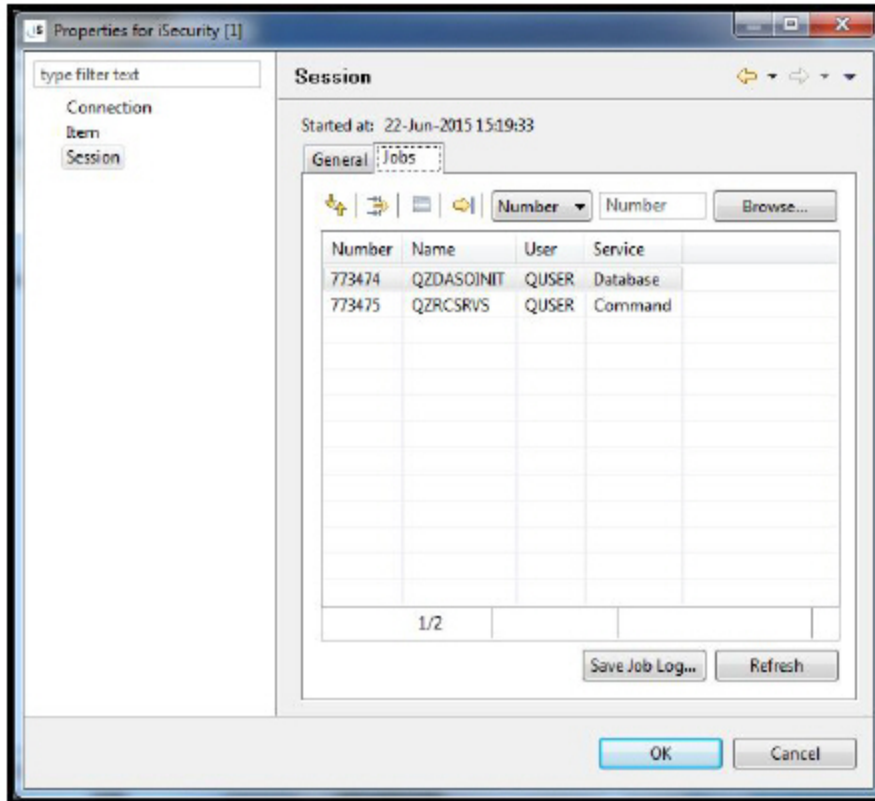
If you have problems with your session, you can highlight the job, click Save Job Log and save the full log to a local computer. This will help support staff to solve your problems.

Navigator

Navigate between the open editor screens according to the order in which they were opened.
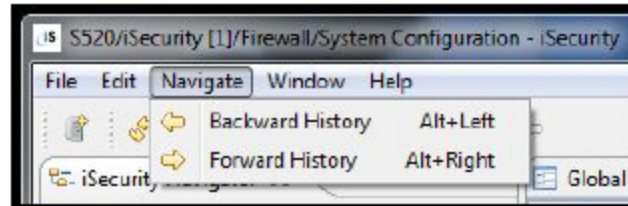
Window

Show View

Display the GUI application possible views.

Go to **Window -> Show View** and select a view to display in the interface layout.
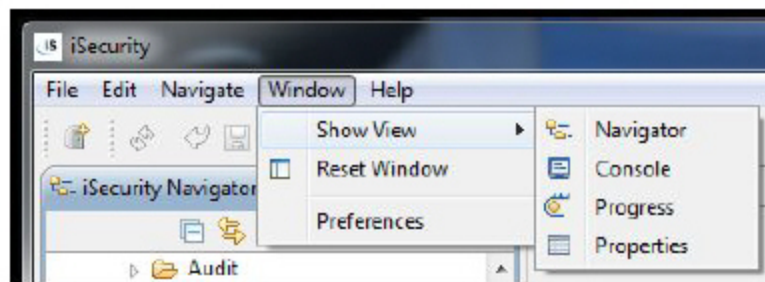
Reset Window

To restore the Window to its default state, click **Reset Window** in the toolbar.
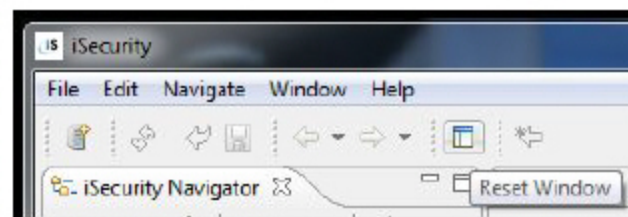
Editors

The navigator node icons are differently designed according to what they display, as shown in the table below:

Icon	Description
	Table
	Form
	External window

Click the **Open Editors** tool bar button to search for an editor name, prefix, or pattern.
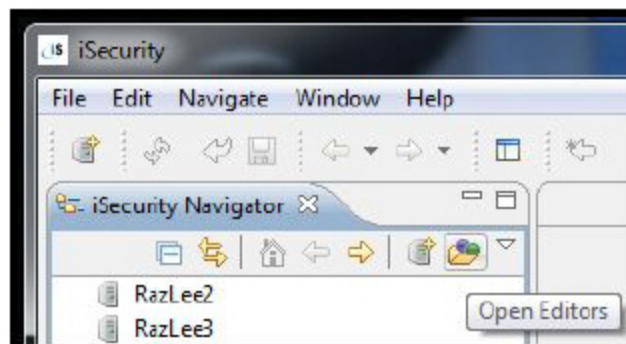
A list of editors are displayed in alphabetic order.
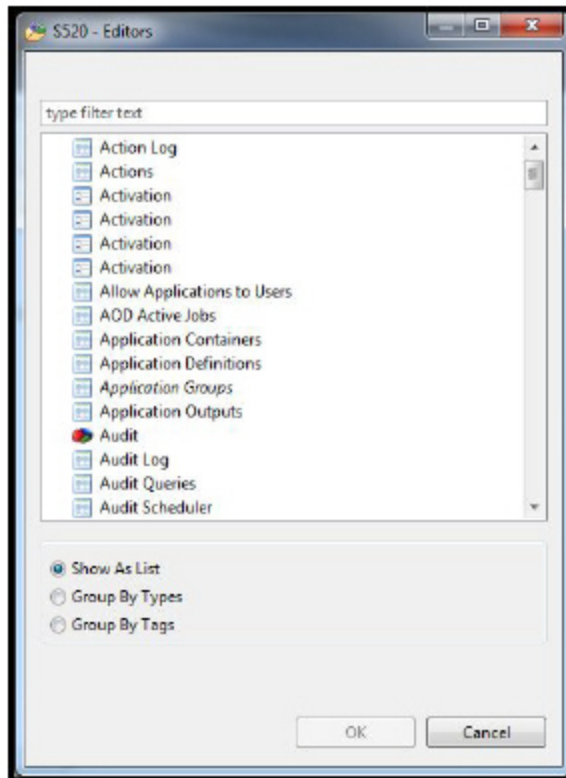
You can also list group the editors by types or by tags.

Nodes with filter

The following example use the **Profiles** node under **User Management**

To filter information, right-click the node and select Properties from the menu. The **Properties for Profiles** dialog displays, select **Filter**.

NOTE: Changes done here will take place at the next attempt to open the editor or at the next attempt to refresh an already opened one.
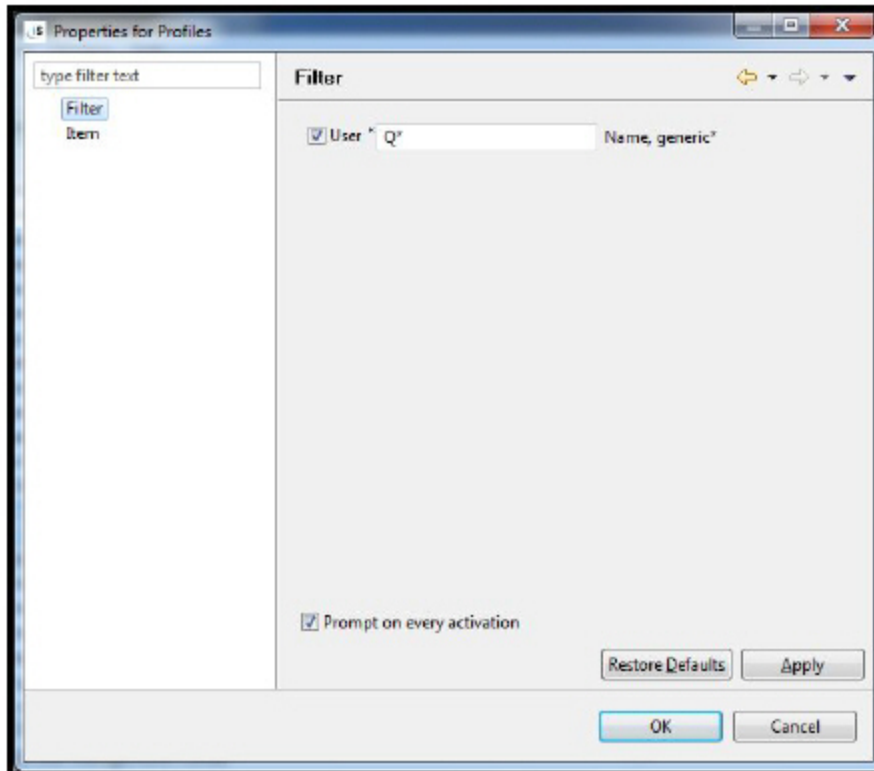
In the example shown, only profiles that start with the letter Q appear. However, users are prompted every time to allow them to change the filter. The filter is also accessible from the editor pop up.

Show entry content

Right-click on any row in a table and select **Show Content** to show a vertical view of the selected entry. This view is the default view if the table has no **Open** button.
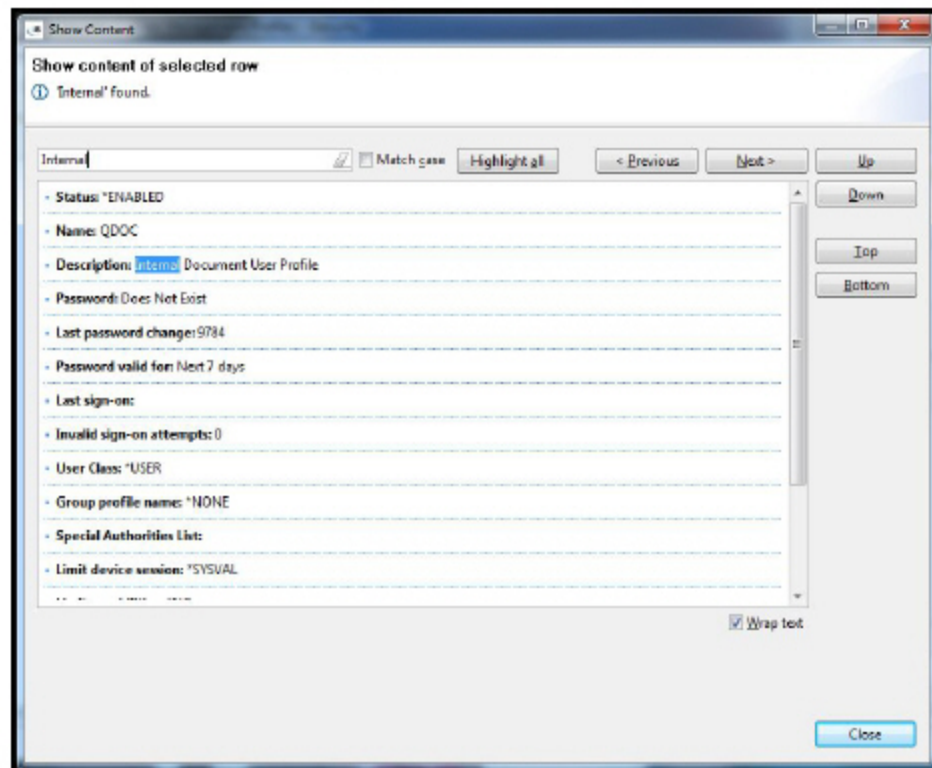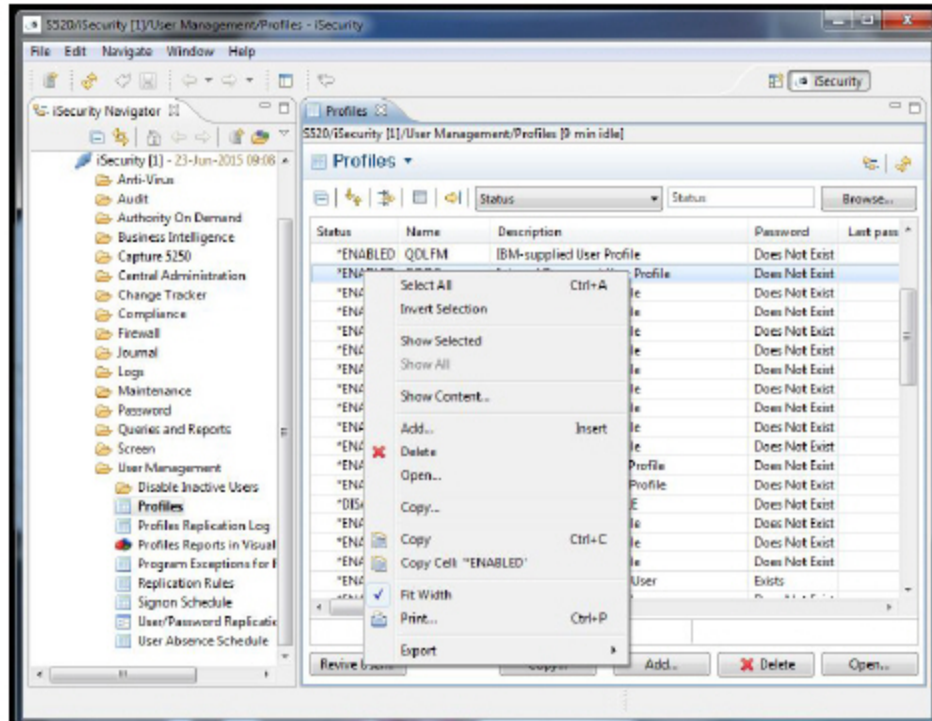
nUse the navigation buttons at the right to navigate the entries.
nUse the search bar at the top of the dialog. The search string is highlighted.

Show Selected Content

There may be occasions when you want to display a selection of the entries in the table, but the entries have no common information that allows you to create a unique filter.

1. Select the required entries and right click on one of them.
2. Click **Show Selected** in the menu. The table is redisplayed with only the selected entries.
3. To return to the display of all the entries, right-click on one of the entries and click **Show All** in the menu.
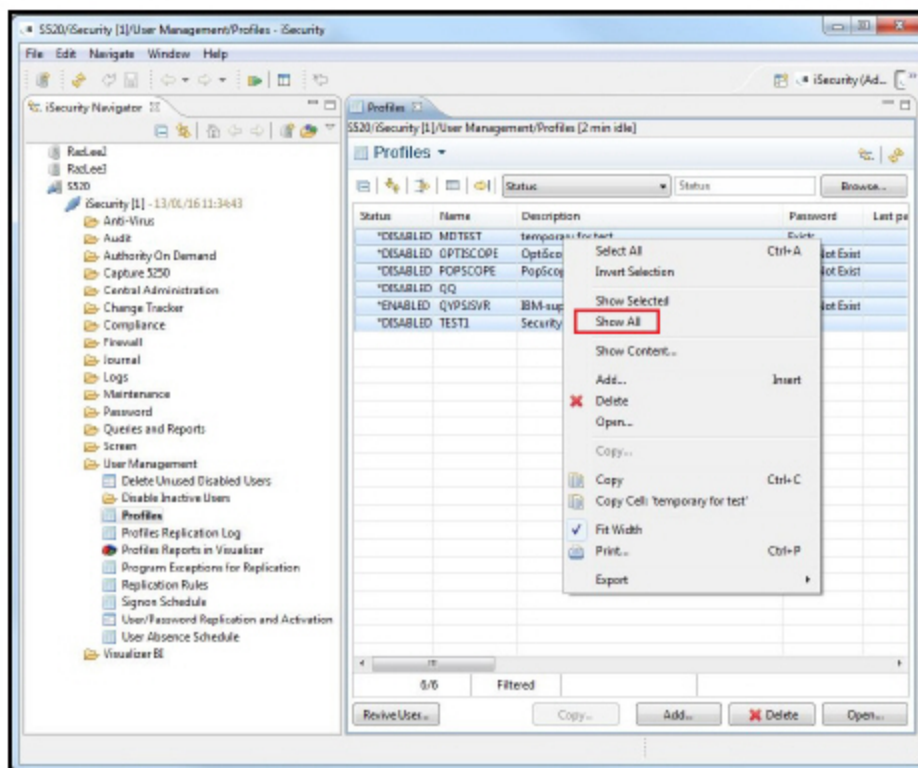
Update

Check for updates in one click

Updates and new releases are available through the GUI itself.

1. Click **Help** -> **Check for Updates**.

2. 2.The GUI connects to the update site. If an update is available, it is installed.

Automatic and Scheduled Updates

If you prefer, you can set the system to check automatically for available updates, the frequency with which to check and also the behavior of the system when an update is detected.

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **Install/Update -> Automatic Updates**.
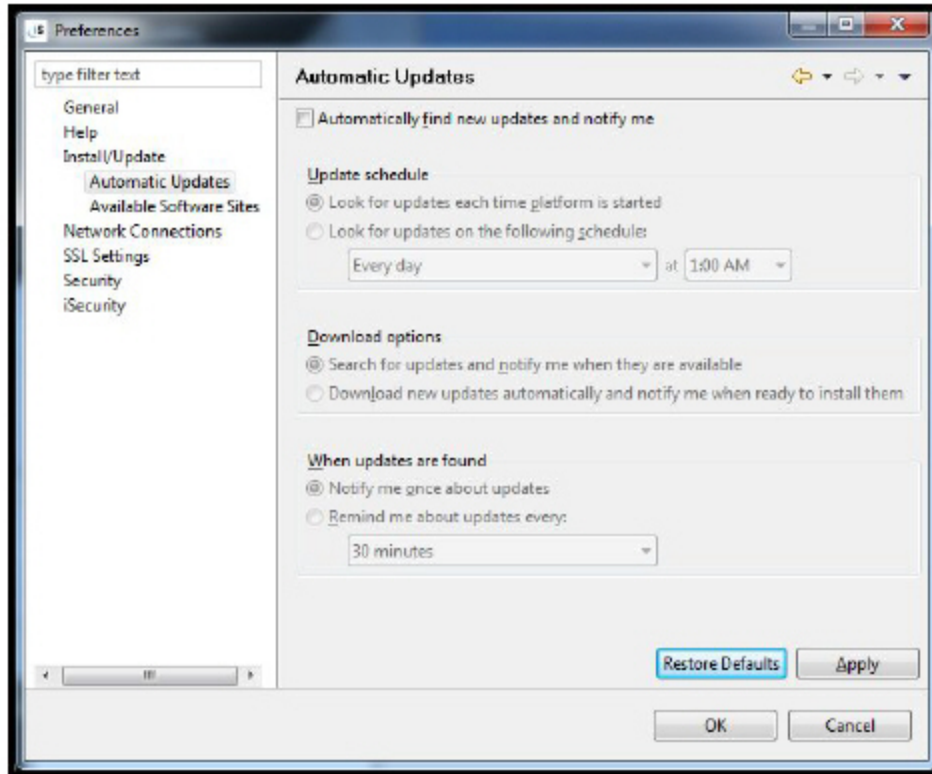
3. Select the **Automatically find new updates and notify me** check box, enter the other parameters according to your requirements, and click **OK**.

Parameter	Description
Update schedule	Select one of these options: • Look for updates each time platform is started • Look for updates each time platform is started If you select **Look for updates on the following schedule**, select a day and time from the drop down lists.
Download options	Select one of these options: • Search for updates and notify me when they are available • Search for updates and notify me when they are available

When updates are found	Select one of these options: • Notify me once about updates • Notify me once about updates If you select **Remind me about updates every**, select a notification frequency from the drop down list.

iSecurity Archived Update Site

If you do not have an internet connection, you can update the application using a local update site.

1. Ask for the new update zip file from your distributor and save it on your local disk.
2. Click **New Archived Site**.
3. In the **Select file** dialog, point it to the location of the zip file supplied to you.
4. In the **Edit Local Site** dialog, click **OK**.

Reporting problems in iSecurity GUI

The iSecurity GUI module writes output to a log file. By default, problems are written to the log file which should be emailed to support@razlee.com.

Log Preferences window

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **iSecurity -> Log**.
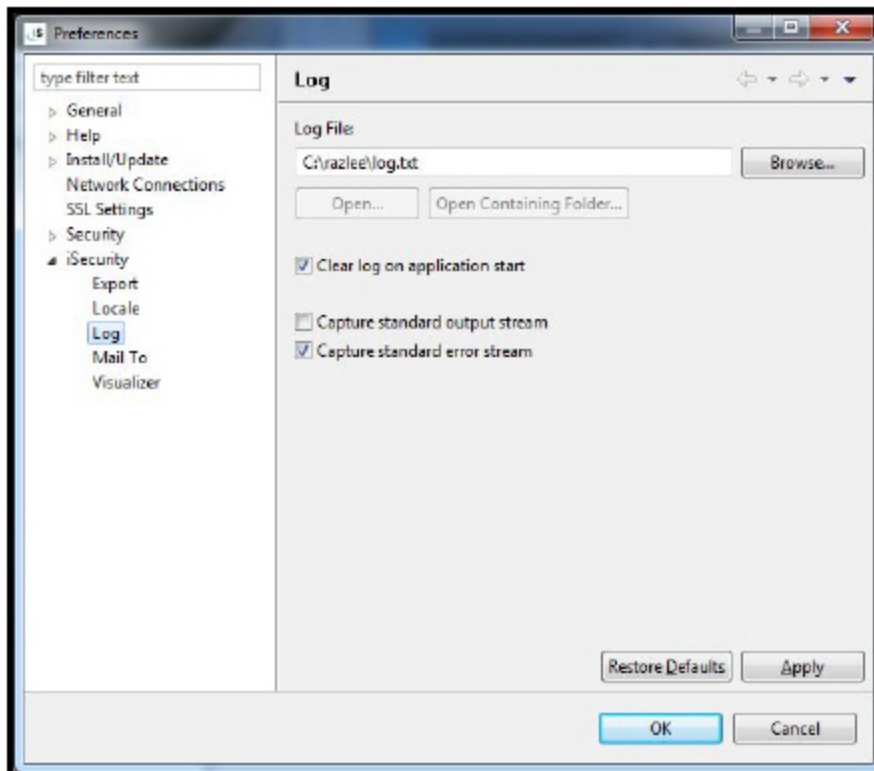
NOTE: Changes made on this screen take effect only after iSecurity is restarted. By default, the log file is cleared when iSecurity starts and only errors are written to it.

You may be asked by the Raz-Lee Technical Support team to select the **Capture standard output stream** check box, recreate the error, and then resend the log file to the support team at support@razlee.com.

Parameter	Description
Open	Opens the log file using the default text

-

	editor
Open Containing Folder	Useful if you wish to send the file as an attachment
Browse	Set a different log file location and name

View Job Log Entries

A job error may trigger an error message alert.
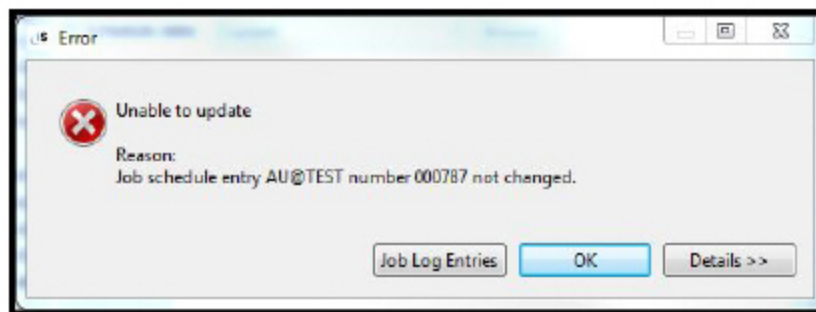
Click the **Job Log Entries** button to view the last ten records of the job log.
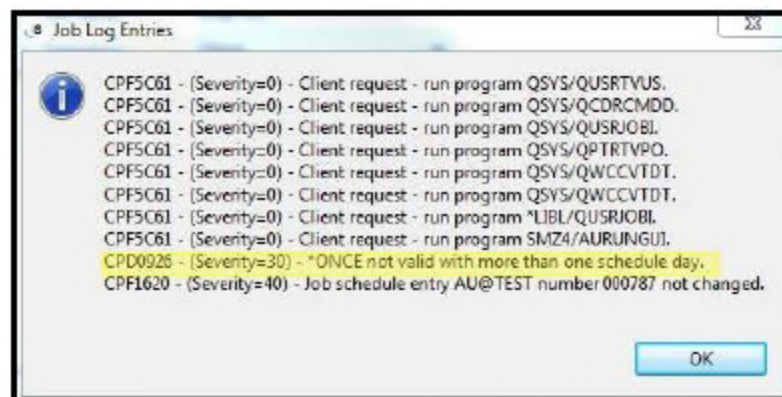
Console

To display in real-time everything the application writes to the log:

1. Click **Window -> Show View -> Console**. The console view is displayed.

Help

A new Help contents is available in an HTML format that support links and bookmarks for easier navigation. The Help also supports a search engine.

Define Help Settings

You can define how you view this help.

To set the Help default settings:

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **Help**.
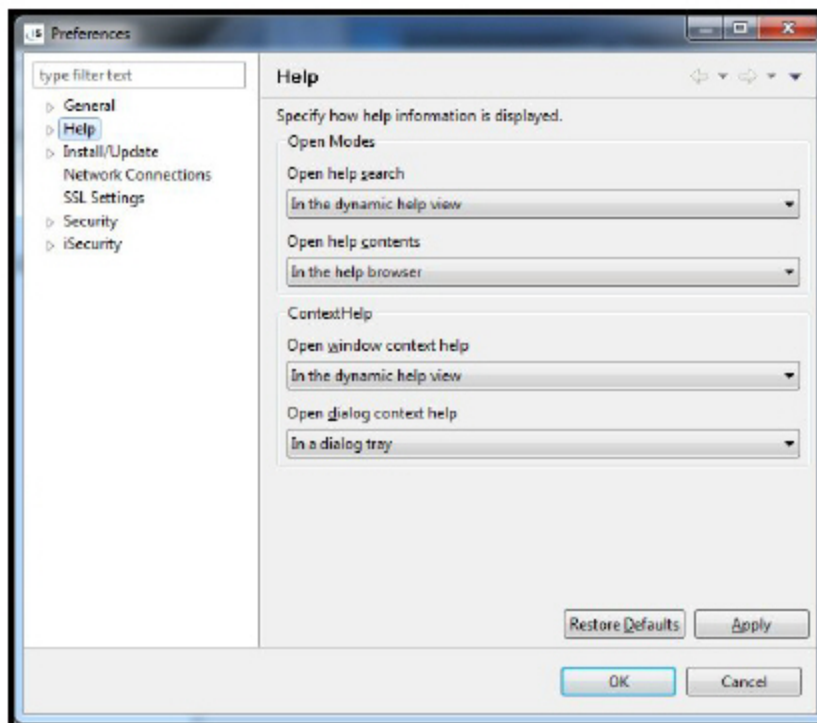
Parameter	Description
Open help search	In the dynamic help view In a browser
Open help contents	In the help browser In an external browser
Open window context help	In the dynamic help view In an infopop

Open dialog context help	In a dialog tray In an infopop

Editors

Information is displayed in tables, forms, tools, windows, and so on that are called editors. This section describes the various functions available to you in the editors.

Every form has both **Save** and **Revert** actions, at both the top and the bottom of the form.
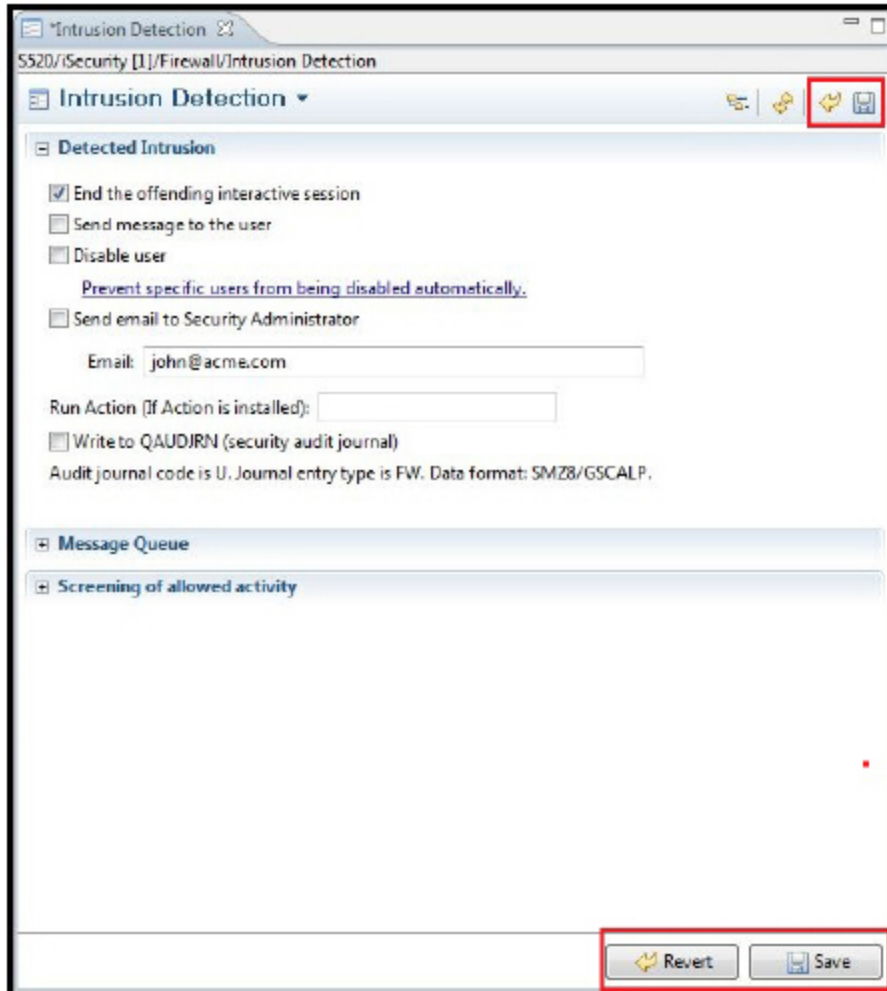
Editor actions are available also via a pop-up menu. Click the down arrow next to the form name to access the pop-up menu.
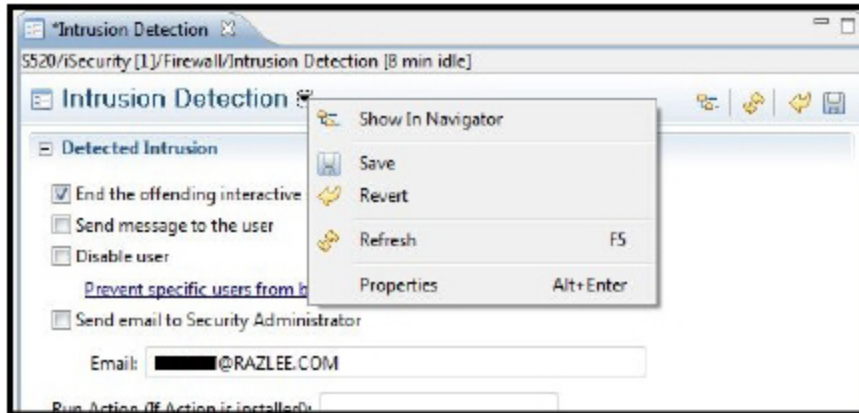
Error messages within the editors are displayed as links
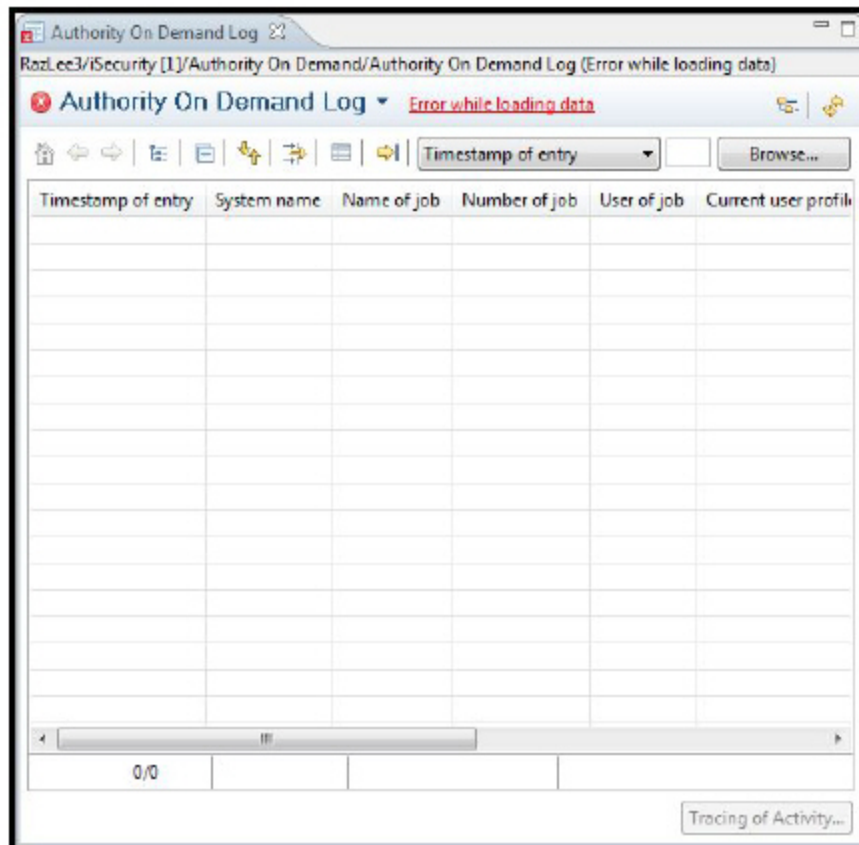
Click the link to display the error message.

Last Modified Editor

The **Last Modified Editor** icon displays/re-opens the last form that was changed. If there are changes waiting for update, the icon displays with a green asterisk.
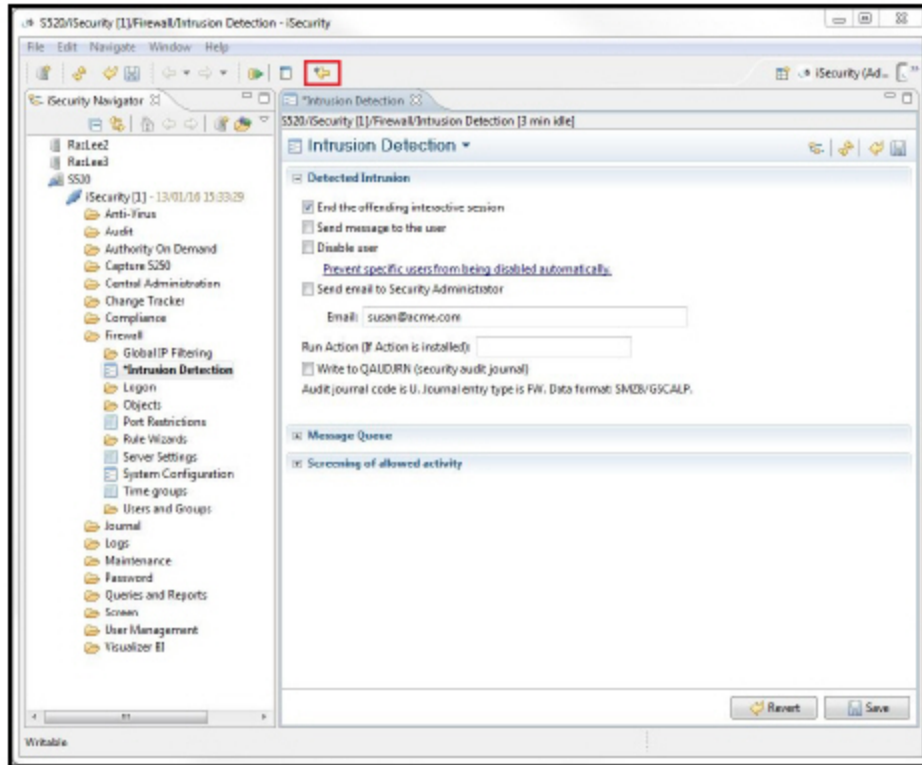
Editor Display

The Editor displays the product name and idle time (where relevant) on both forms and tables.

Print format

Right-click on a record or several records to print in the following printing formats:

- Excel 2003 XML format
- Open Document Format Spreadsheet
- Hypertext Markup Language (HTML)
- Portable Document Format (PDF)
- Comma Separated Values (CSV)
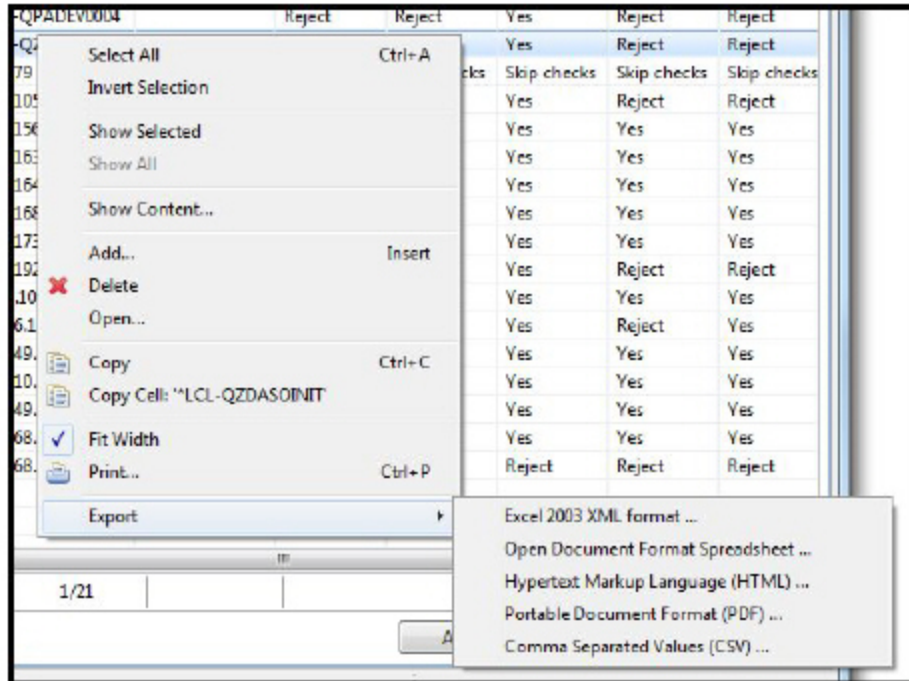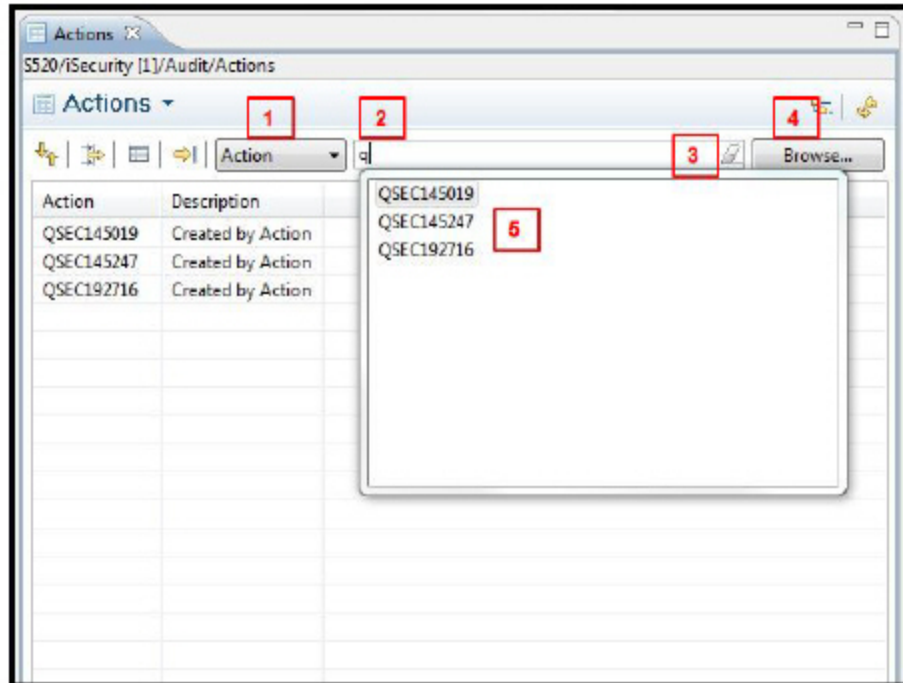
Open Editor Display

Even if you are unable to see all open editors, a quick look at the Navigator pane shows you which editors are open, which editors are open and have had changes made, and which editors were open in this session and have now been closed. Open editors are displayed in bold, open editors with unsaved changes are displayed in bold with an asterisk to the left of the editor name, and closed editors are displayed in italics.

In the example, the **Incoming IP Addresses** and **Incoming Remote System Names** editors are open, the **Intrusion Detection** editor is open with an unsaved change (indicated by the asterisk), and the **Outgoing IP Addresses** editor was open and has now been closed.
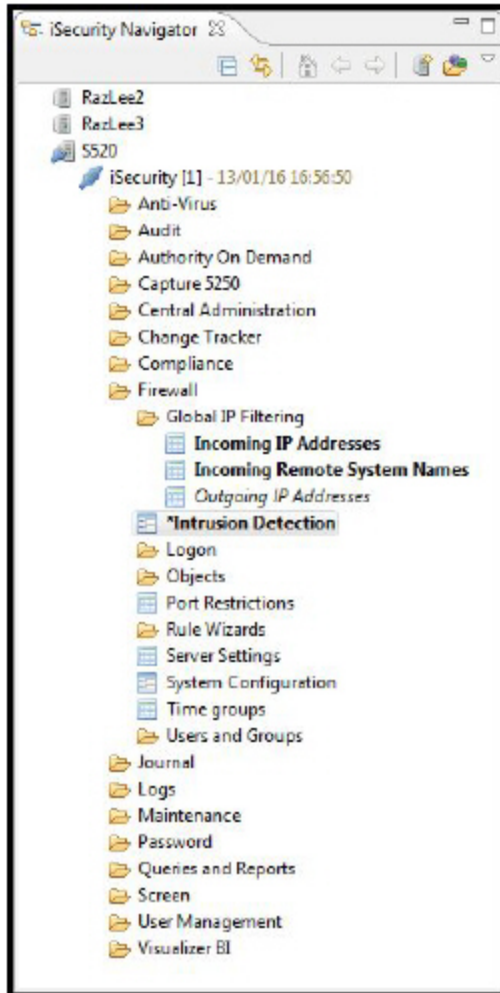
Table Filter

All table editors have a built in filter that also suggests filter criteria. For an explanation of the functionality of the filter, see the table below.
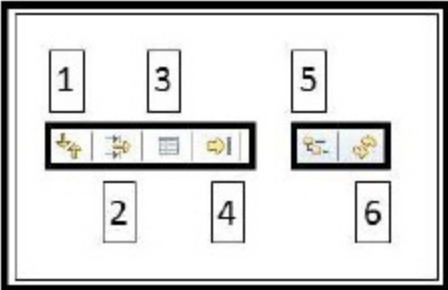
Number	Description
1	You can filter the display on any of the fields in the table. Choose the field you want from this drop down list. The default field is the first field of the table.
2	Type your search here. You can search for specific strings, or you can use substitution characters, an asterisk (*****) for any string of any length and a question mark (**?**) for any single character. You can also search for filter for a string with a specific ending by typing less than (**<**) after the last character. To search for the actual characters used as substitution characters, type a back slash (****)before the character.
3	Click the **Clear** icon to remove your search.
4	Click **Browse...** to open the **Choose Value** dialog, based on the input. Select one of the values and

	click **OK**.
5	Displays the values which match your current filter.
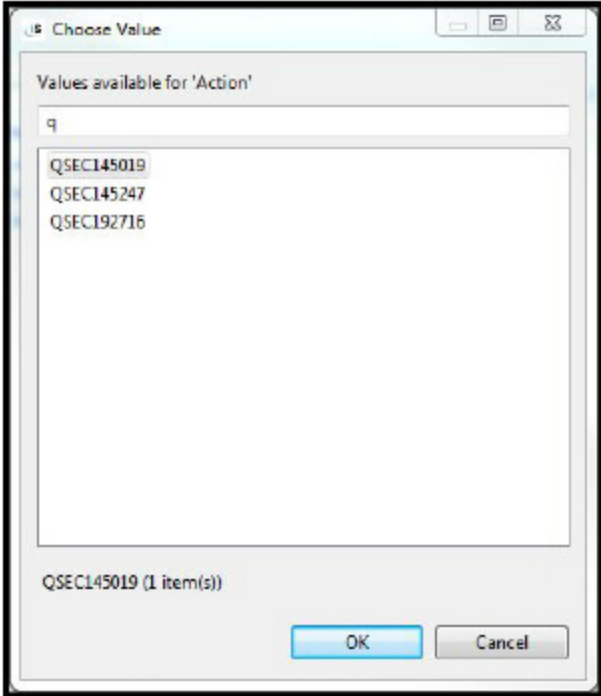
Editor Toolbars

The numbers in the descriptions below refer to the call-out numbers in the screenshot.

Sort (1)

Opens the **Sort by columns** dialog that enables you to define how the table will appear in the current session. You can define the order in which the fields will be sorted and if individual fields will be sorted ascending or descending.

Filter (2)

Opens the **Filter** dialog that enables you to define a subset of the members of the table.

Visible Columns (3)

Opens the **Hide/Show table columns** dialog that enables you to define which columns will appear in the table in the current session.
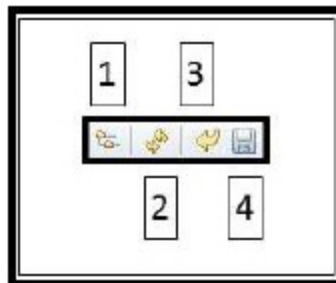
Pack Columns (4)

Sets all columns in the table to their optimal size.

Show in Navigator (5)

Puts the cursor on the entry for the table in the Navigator Pane.

Refresh (6)

Refreshes the contents of the open Editor without closing it. If any work has not been saved, a warning message is displayed.

The numbers in the descriptions below refer to the call-out numbers in the screenshot.

Show in Navigator (1)

Puts the cursor on the entry for the table in the Navigator Pane.

Refresh (2)

Refreshes the Session without closing it. If any work has not been saved, a warning message is displayed.

Revert (3)

Reverts any changes that have not yet been committed.
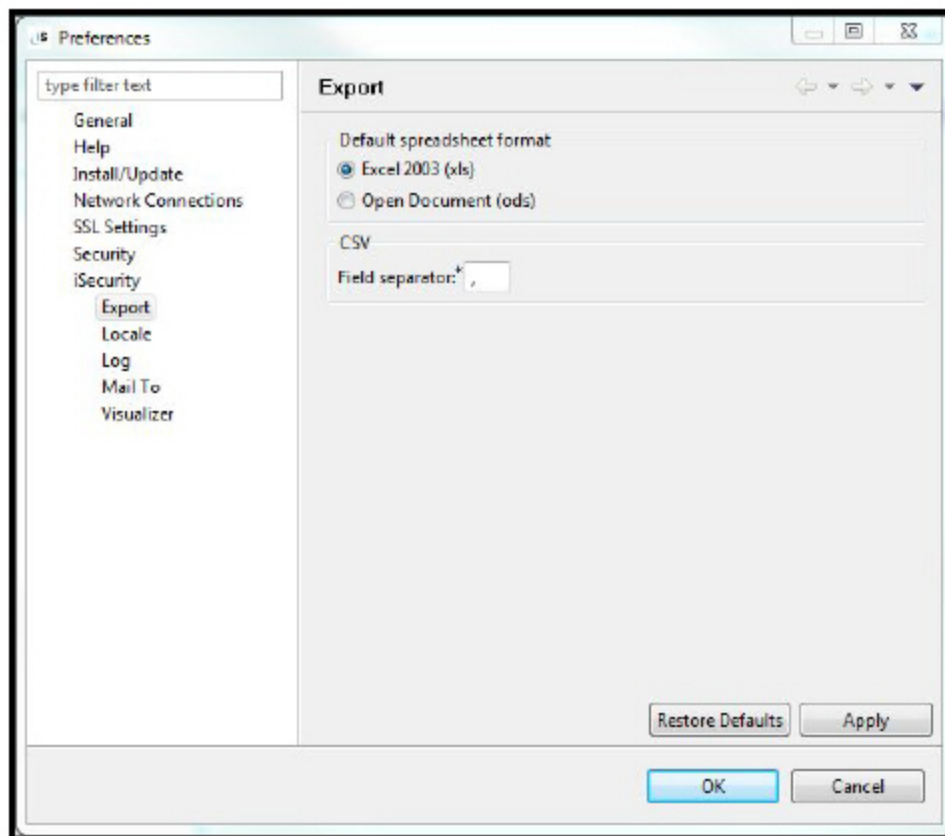
Save (4)

Saves all changes.

Preferences

Use the **Preferences** window to define how you want to work with the iSecurity GUI.

Export

To define the field separator for CSV outputs such as Excel or Open Document (used in the logs):

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **iSecurity -> Export**.
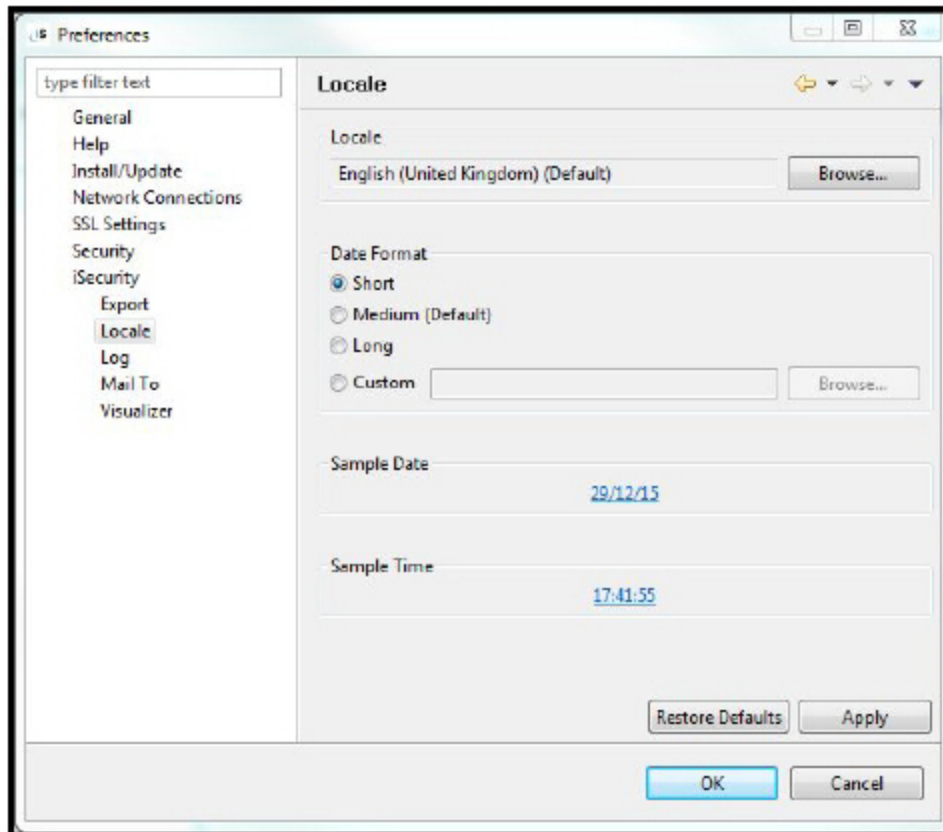

Locale

The locale defines the way the local time and date are displayed.

The locale (like all other preferences) is defined for the Workspace. If you need to use different locales for different computers, you need to define additional Workspaces. See Switch Workspace for more details.

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **iSecurity -> Locale**.

3. Click **Browse...** in the **Locale** field to select the language and country that control which date formats are available.
4. Select the **Date Format** for your organization.
5. Click **OK**.

Mail To

To define a default Email address to be used in queries, compliance and scheduler:

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **iSecurity -> Mail To**.
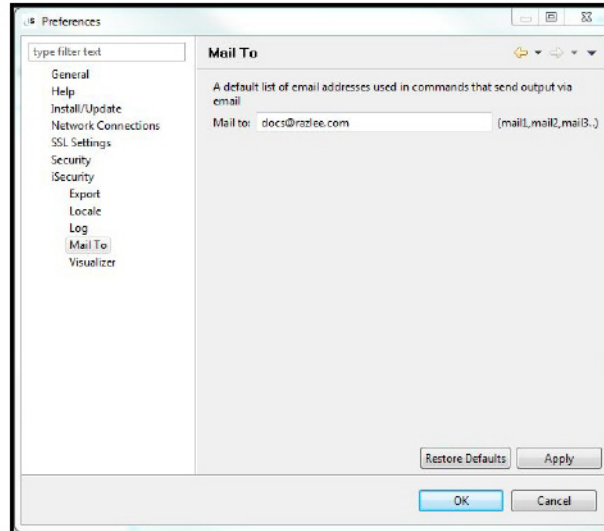
3. Enter the email address to be used. You can enter as many addresses as required; they should be separated by a comma (for example: john@acme.com, susan@acme.com, ceo@acme.com).

4. Click **OK**.

Visualizer

Statistical data for Visualizer is collected in a daily maintenance job that runs overnight. You can define that Visualizer statistical data is collected more frequently than that.

1. Click **Window -> Preferences**. The **Preferences** dialog is displayed.
2. In the navigation pane, select **iSecurity -> Visualizer**.
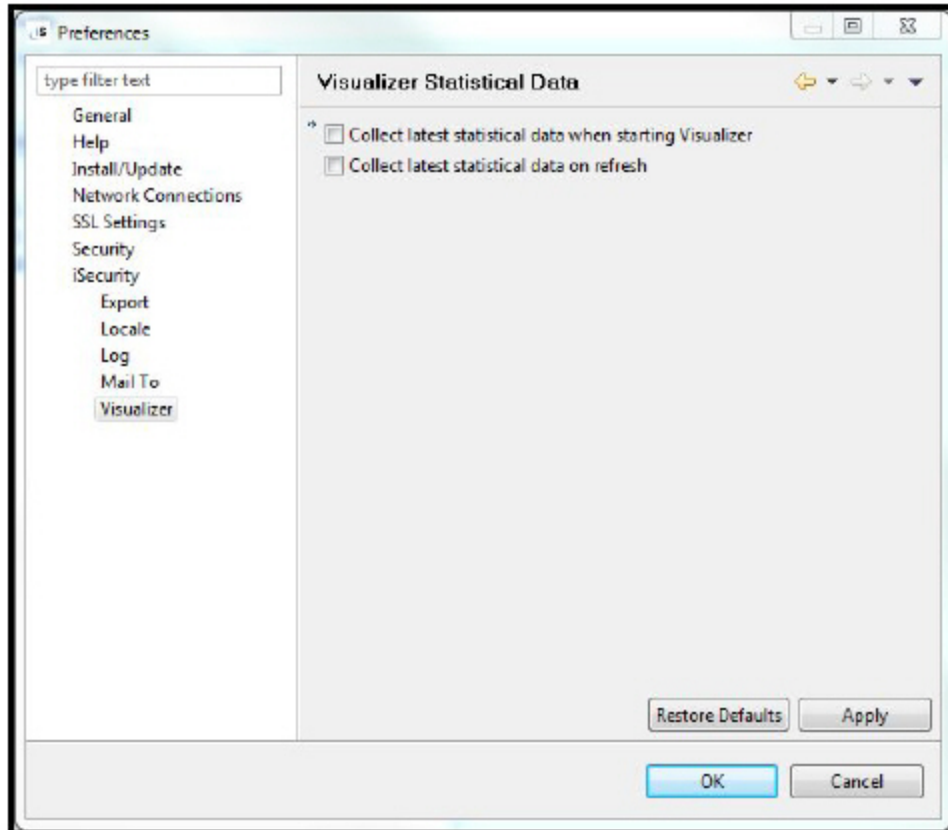
3. Select **Collect latest statistical data when starting Visualizer** to update the data every time an instance of Visualizer is opened.

4. Select **Collect latest statistical data on** to enable Visualizer to reload data from the database instead of using cache when requested.
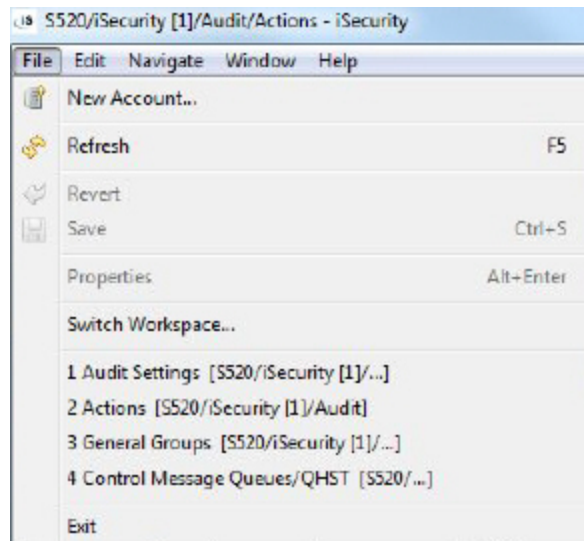
NOTE: You can update Visualizer manually whenever required, by using the Add Latest Data option in the Visualizer Maintenance form. See Maintaining the Visualizer BI Data for more information.

Standard Functionality

This section describes the standard functions of the various menus and toolbars that are available in the iSecurity GUI.

File Menu

New Account

Opens the Account Wizard. See Create a New Account for more details.

Refresh

Refreshes the Session without closing it. If any work has not been saved, a warning message is displayed.

Revert

Reverts any changes that have not yet been committed.

### Save

Saves all changes.

Properties

Displays the **Properties** dialog related to where the cursor is situated.

Switch Workspace

iSecurity GUI allows you to work in more than one workspace. You may want to do this to have a different set of preferences for different work purposes; for example to use different locales for different accounts. The default workspace that is built when you run iSecurity for the first time is in a directory that is placed in the user's home directory (usually **C:\Users**<UserName>**).

1. Select **Switch Workspace...** The **Select a Workspace** dialog is displayed.
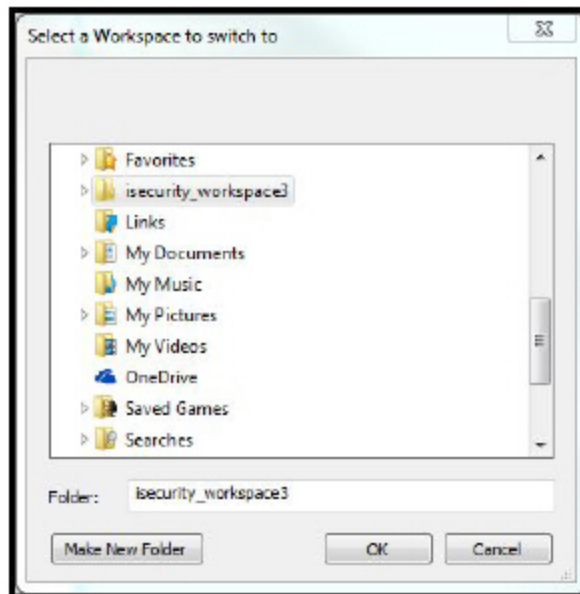
2. Select an existing directory or click **Make New Folder** to create the Workspace directory.
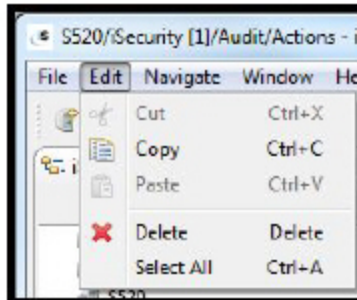3. Click **OK**. You are now working in the new Workspace.

NOTE: All future sign-ons to iSecurity will be in the new Workspace until you change back.

Recent Editors

A list of up to the last four editors is shown. Click on one of the entries to go directly to that editor.

Edit Menu

The Edit Menu gives you an additional place from which to use standard editing functions.

Navigate Menu

The Navigate Menu allows you to go backwards and forwards between the various editors you have recently worked on, using the **Backward History** and **Forward History** options. You can also use the **Open Node** option to open a dialog that allows you to see all the nodes available in the session and open a specific node without knowing its place in the navigation tree.
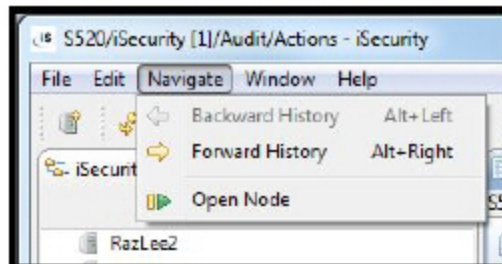
Backward History

Click **Backward History** to return to the Editor you were working on immediately before the current Editor.

Forward History

Click **Forward History** to return to the Editor from which you came to the current Editor.

Open Node

Click **Open Node** to open the **Open Node** dialog. You can scroll to the node you want or you can search for it in the search box. You can search for specific strings, or you can use substitution characters, an asterisk (*****) for any string of any length and a question mark (**?**) for any single character. You can also search for filter for a string with a specific ending by typing less than (**<**) after the last character. To search for the actual characters used as substitution characters, type a back slash (****)before the character.

Window Menu
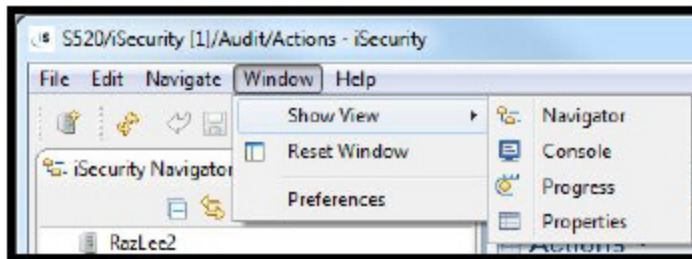
Show View

Click **Show View** to open one or more of the **Navigator**, **Console**, **Progress**, or **Properties** panes.

Reset Window

Click **Reset Window** to close all panes that you opened using **Show View**.

Preferences

Click **Preferences** to open the **Preferences** dialog. More information about the various options can be found throughout this section.

Help Menu

The help menu allows you to open the Online Help, to check for and install updates to the software, to display the version and build information, to display the copyright information, and to open the installation Details dialog.
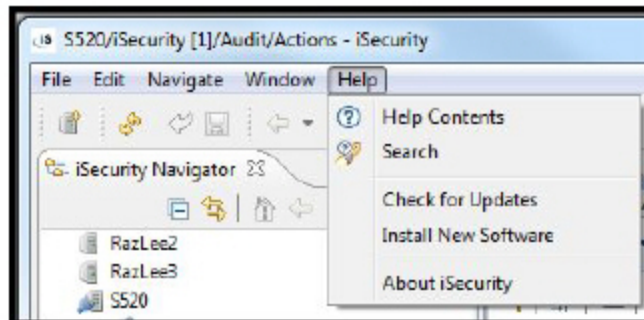
## Help Contents

Click **Help Contents** to open the Online Help.

Search

Click **Search** to open a dialog that allows you to search for keywords in the Online Help. All topics in which the keyword appears in the search results pane.
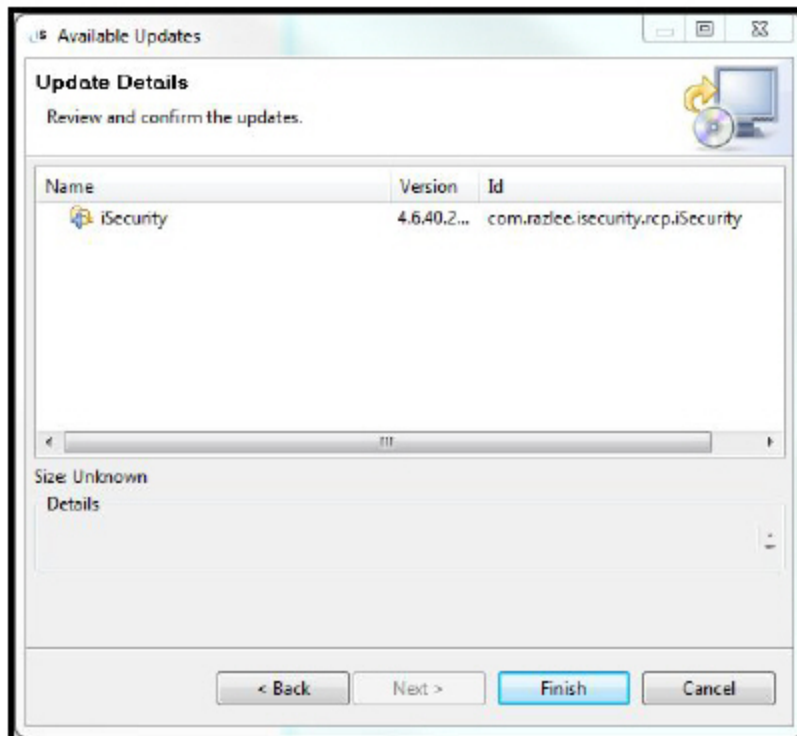
Check for Update

1. Click **Check for Updates** to check if there is a new version of the software available. If there is, the **Available Updates** dialog is displayed.
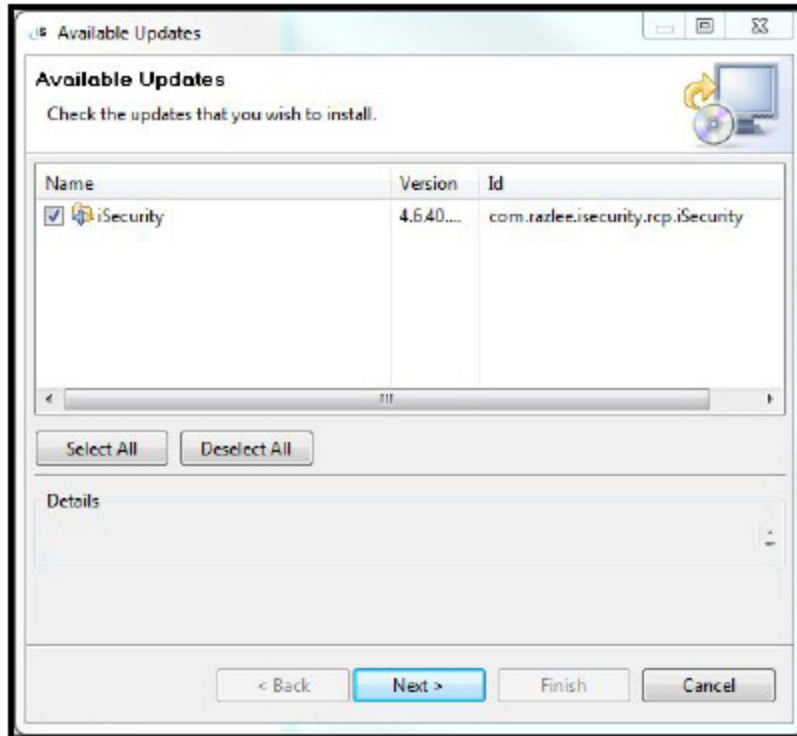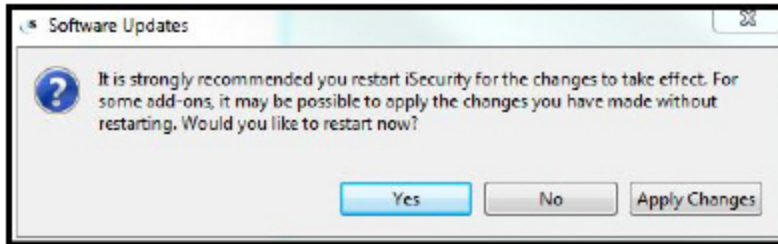
2. Click **Next**. The **Update Details** dialog is displayed.

3. Click **Finish**. The update runs.
   When the process completes, the **Software Updates** dialog is displayed.

4. Click **Yes** to restart iSecurity.

About iSecurity

Click **About iSecurity** to open the **About iSecurity** dialog. This dialog shows you the version and build of your iSecurity installation, gives you a link to the RazLee website, and allows you to open the **Installation Details** dialog.


The **Installation Details** dialog has four tabs; **Installed Software**, **Installation History**, **Plug-ins** and **Configuration**. Only the **Installation History** tab is important for users, because it is used when you want to revert to a previous version of the software.

Revert to a Previous Version

For various reasons, you may need to revert to a previous version of the software. Before you do this, you should ensure that the download file of the

software is in the directory that you defined in [iSecurity Archived Update Site](#).

1. Click **Installation Details** in the **About iSecurity** dialog. The **Installation Details** dialog is displayed.
2. Select the **Installation History** tab.
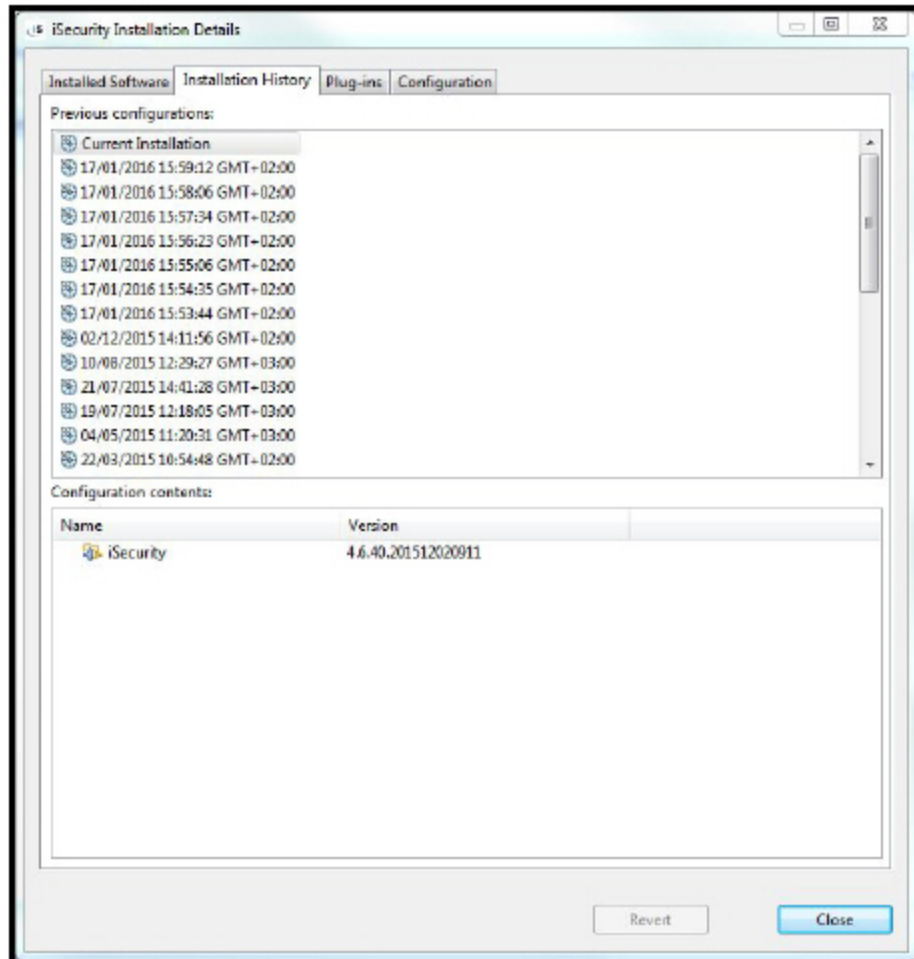
3. Select the version you want to revert to and click **Revert**.
4. Click **Yes** in the **Revert Software Configuration** dialog. The **Revert Configuration** dialog is displayed.
5. When the process completes, the **Software Updates** dialog is displayed. Click **Yes** to restart iSecurity.

Account Menu

To access the account menu, right click on the account.
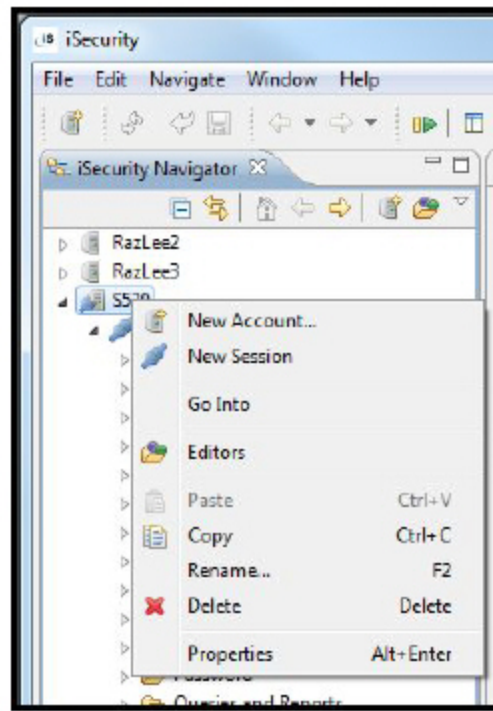
New Account

Opens the Account Wizard. See Create a New Account for more details.

New Session

Opens the New Session Connection dialog to allow you to open a new session for this account. See Sessions for more details

Go Into

Hides everything in the navigation pane except this Account. All other Accounts are hidden. Click **Go back** in the Navigator toolbar to return to the previous display.

Editors

Opens an alphabetical list of all the Editors currently available for this account. If you have more than one session open, an entry for the editor will

appear as many times as there are open sessions, in the order of the open sessions.

Paste

Allows you to create a new Account with the identical properties of a copied Account.

Copy

Copy the Account to open a new Account with identical properties
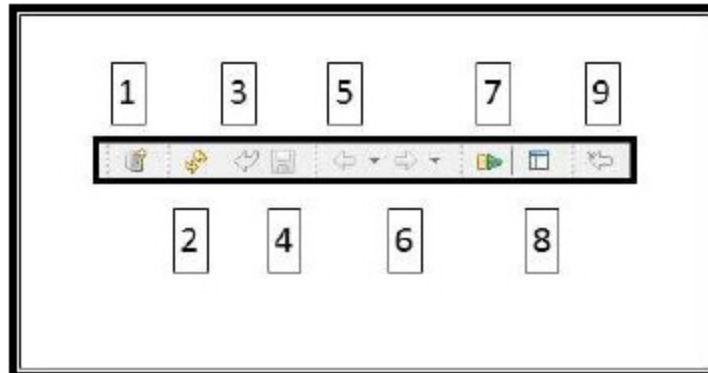
Rename

Rename the account

Delete

Delete the account.

Properties

Opens the **Properties** dialog for the Account. See [Account Information Properties](#) for more details.

iSecurity Toolbar

The numbers in the descriptions below refer to the call-out numbers in the screenshot.

New Account (1)

Opens the Account Wizard. See Create a New Account for more details.

Refresh (2)

Refreshes the Session without closing it. If any work has not been saved, a warning message is displayed.

Revert (3)

Reverts any changes that have not yet been committed.

Save (4)

Saves all changes.

Back (5)

Returns to the Editor you were working on immediately before the current Editor.

Forward (6)

Returns to the Editor from which you came to the current Editor.

Open Node (7)

Opens the **Open Node** dialog. You can scroll to the node you want or you can search for it in the search box. You can search for specific strings, or you can use substitution characters, an asterisk (*****) for any string of any length and a question mark (**?**) for any single character. You can also search for filter for a string with a specific ending by typing less than (**<**) after the last character. To search for the actual characters used as substitution characters, type a back slash (****)before the character.

Reset Window (8)

Closes all panes that you opened using **Show View**.

Last Modified Editor (9)

Displays/re-opens the last form that was changed. If there are changes waiting for update, the icon displays with a green asterisk.

Navigation Pane Toolbar
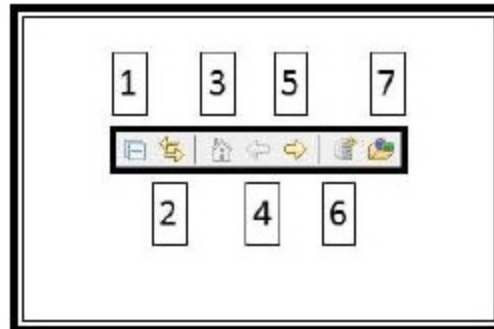
The numbers in the descriptions below refer to the call-out numbers in the screenshot.

Collapse All (1)

Collapses all open nodes in the Navigation Pane.

Link with Editor (2)

Opens the **Navigation Pane** to the node of the current tab.

Home (3)

Reverts the action of all uses of the **Go Into** icon.

Back (4)

Reverts the action of the last use of the **Go Into** icon.

Go Into (5)

Hides everything in the navigation pane except this Account/Session. All other Accounts/Sessions are hidden.

New Account (6)

Opens the Account Wizard. See Create a New Account for more details.

Open Editors (7)

Opens an alphabetical list of all the Editors currently available for this account. If you have more than one session open, an entry for the editor will

appear as many times as there are open sessions, in the order of the open sessions.

Session Menu

To access the Session menu, right click on the Session.
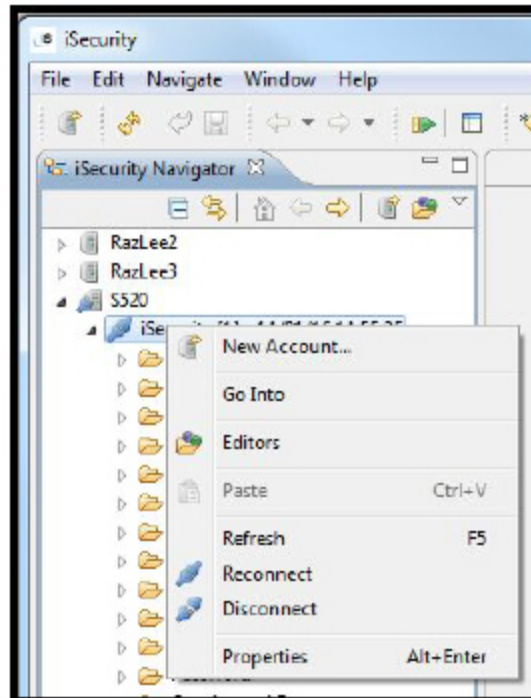
New Account

Opens the Account Wizard. See [Create a New Account](#) for more details.

Go Into

Hides everything in the navigation pane except this Session. All other Sessions for this Account and all other Accounts are hidden. Click **Go back** in the Navigator toolbar to return to the previous display.
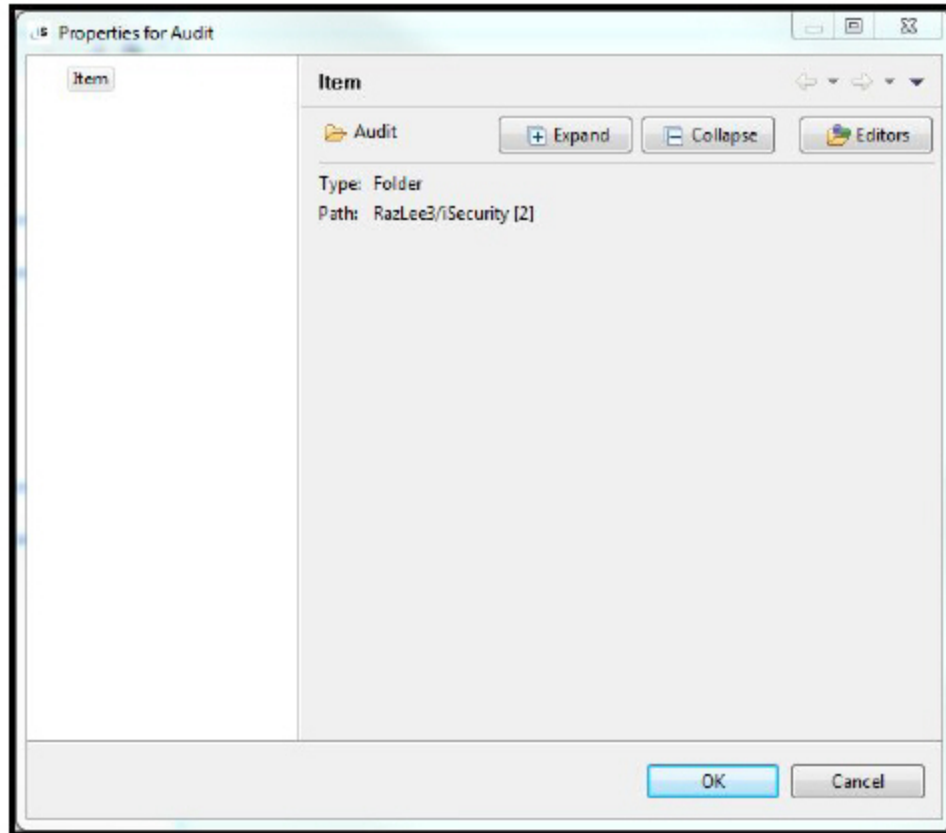
Editors

Opens an alphabetical list of all the Editors currently available for this session.

Paste

Allows you to create a new Account with the identical properties of a copied Account.

Refresh

Refreshes the Session without closing it. If any work has not been saved, a warning message is displayed.

Reconnect

Closes and re-opens the sessions. If any work has not been saved, a warning message is displayed.

Disconnect

Closes and re-opens the sessions. If any work has not been saved, a warning message is displayed.

Properties

Opens the Properties dialog for the Session. See Session Properties for more details.

Folder Menu

To access the Folder menu, right click on the Folder.
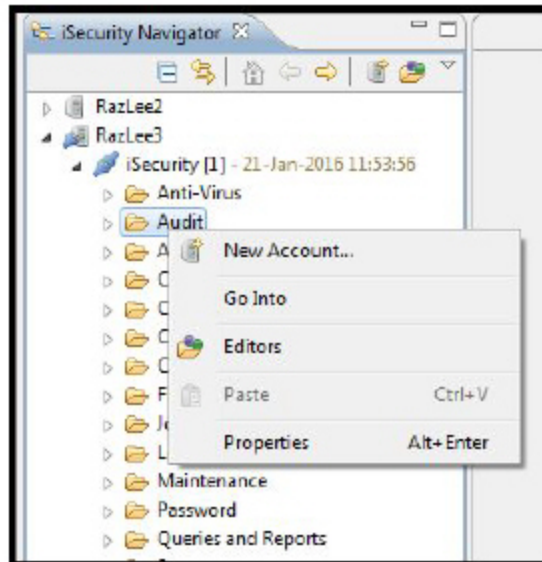
New Account

Opens the Account Wizard. See Create a New Account for more details.

Go Into

Hides everything in the navigation pane except this Folder. All other Folders in this Session, all other Sessions for this Account and all other Accounts are hidden. Click **Go back** in the Navigator toolbar to return to the previous display.

Editors

Opens an alphabetical list of all the Editors available for this folder.

Paste

Allows you to create a new Account with the identical properties of a copied Account.

Properties

Opens the Properties dialog for the Folder.

Click **Expand** to display all nodes available for the folder in the navigation pane.

Click **Collapse** to hide all the nodes of the folder.

Click **Editors** to open an alphabetical list of all the Editors currently available for this folder.

Queries and Reports

Queries

iSecurity comes with hundreds of predefined reports and queries that are ready to run at any time. All reporting features are available to be used both from the GUI and from the green screen. iSecurity GUI also supports Linux queries.

Add a New Query

1. To add a new query, navigate to **Queries and Reports -> Queries**.
2. Double click the node of the type of Query you want to add.
3. Click **Add**. The appropriate **Add Query** wizard is displayed.
4. Use the wizard to create the Query. For an explanation of the fields, see the Queries section in the appropriate User Guide.

NOTE: Do not start the name of a new query with the letter Z. Queries that are supplied by Raz-Lee start with the letter Z. If your queries also start with the letter Z, you will lose them when you upgrade the product.

Modify a Query

1. To modify a query, navigate to **Queries and Reports -> Queries**.
2. Double click the node of the type of Query you want to modify.
3. Select the query you want to modify and click **Open**. The **Edit Query** dialog is displayed.
4. Use the dialog to modify the Query. For an explanation of the fields, see the Queries section in the appropriate User Guide.

NOTE: Do not modify any Queries that were supplied by RazLee. The name of a Query supplied by RazLee starts with the letter Z. Any changes that you may make will be overwritten the next time you upgrade the product. If you want to modify a Query supplied by RazLee, copy it to a new name that does not start with the letter Z, and then modify it.

Copy a Query

1. To copy a query, navigate to **Queries and Reports -> Queries**.
2. Double click the node of the type of Query you want to copy.
3. Select the query you want to modify and click **Copy**. The **Copy Query** dialog is displayed.
4. Enter a new name for the Query and click **OK**. The new Query is added to the list of Queries.

> **NOTE**: Do not start the name of a new query with the letter Z. Queries that are supplied by RazLee start with the letter Z. If your queries also start with the letter Z, you will lose them when you upgrade the product.

5. Use [Modify a Query](#) to make any required changes to the Query.

Reports

Work with Reports

1. Navigate to **Queries and Reports -> Queries**.
2. Double click the node for the type of Query you want to run:
   - Audit
   - Change Tracker
   - Command
   - Compliance
   - Firewall
   - PTF Status
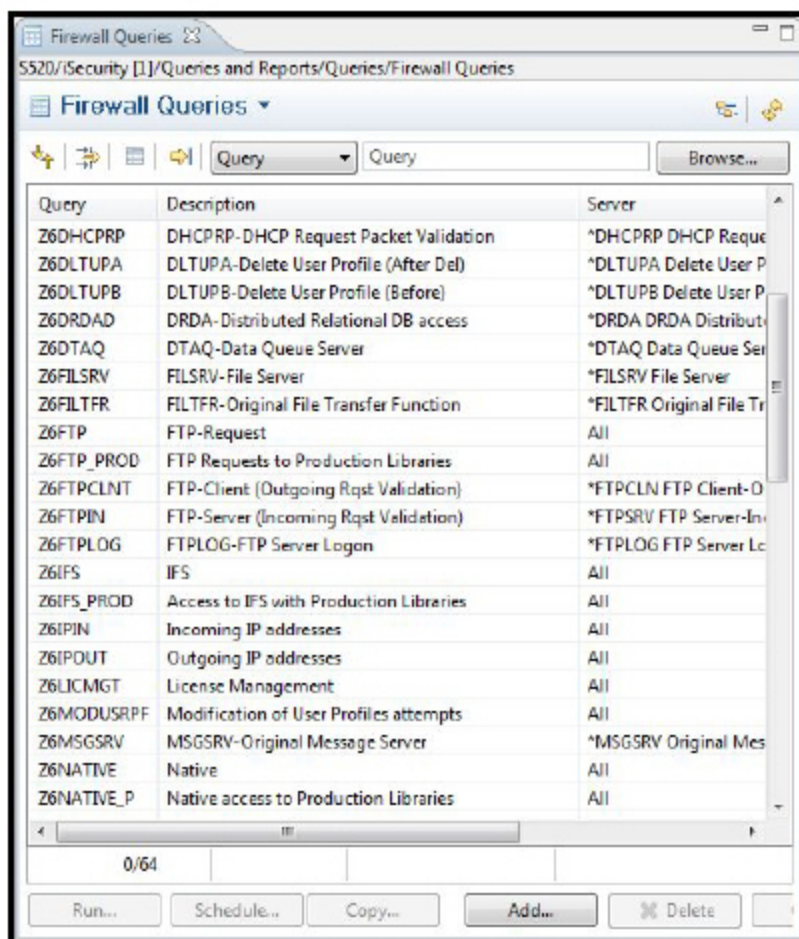
Run a Report

1. Select a query and click **Run**. The **Output Format** dialog is displayed.
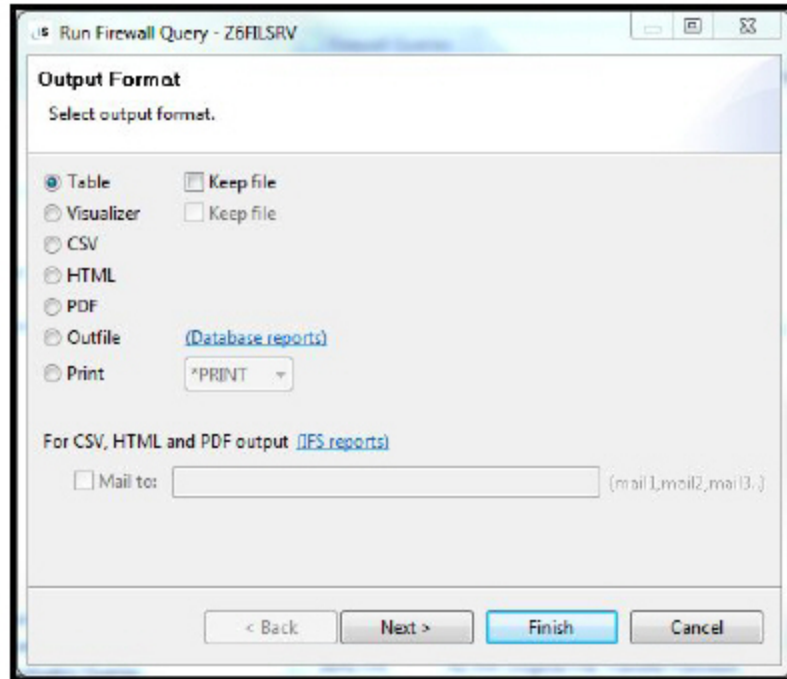
Options/Parameters	Description
Table	The report is output to a Table viewable in the GUI
Visualizer	The report is output directly to Visualizer.
CSV	The report is output to a csv format file and can be sent to an email address.
HTML	The report is output to an html format file and can be sent to an email address.
PDF	The report is output to a PDF format file and can be sent to an email address.
Outfile	The report is sent to an outfile.

Print	The report is sent to one of the designated IBM i printers. Select the printer from the drop down list.
Email Addresses	If you send the report to a csv, html or pdf format, you can also send the report by email. Enter the addresses here.

2. Select the required output format parameters and click **Next**. When relevant, the **Time and Date** dialog is displayed. If it is not relevant, the **Additional Parameters** dialog is displayed. Continue with .
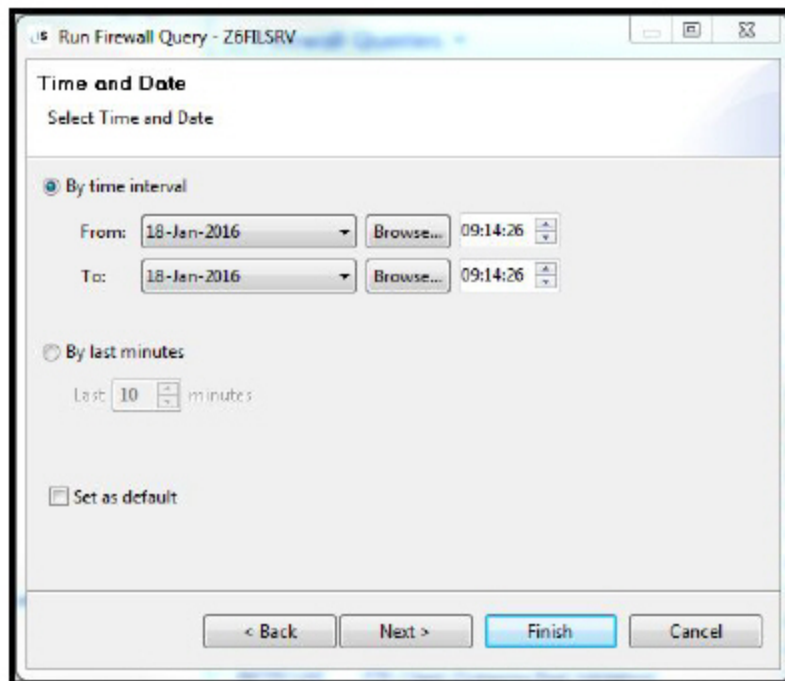
Options/Parameters	Description
By time interval	Select this to enter a time range for the report.
By last minutes	Select this to run the report for a period that just finished. For example, the last 30 minutes.

-

Set as default	Select this to make the time selection the default selection for every time this report is run.

3. Select your time range parameters and click **Next**. The **Additional Parameters** dialog is displayed.
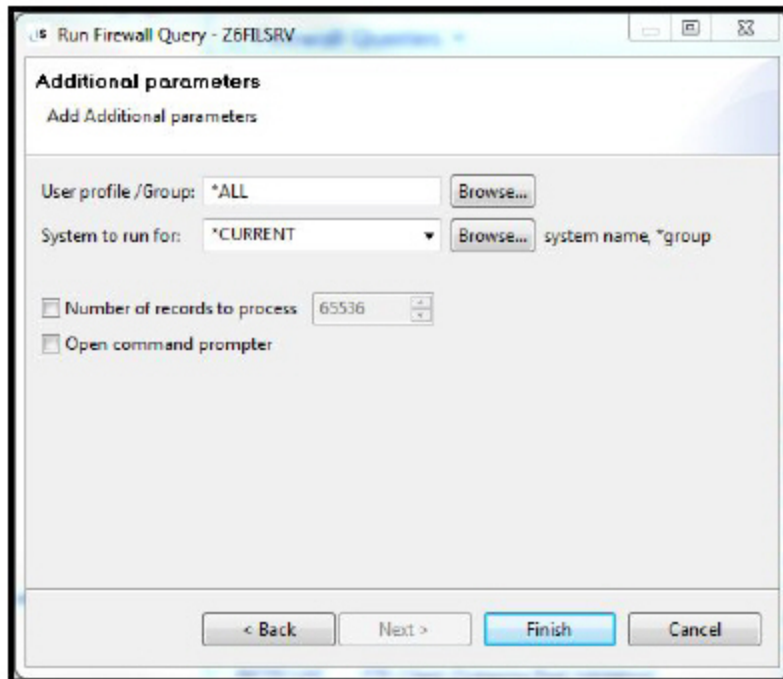
Options/Parameters	Description
User profile/Group	Enter the User/Group Profile for the report. The default is to run the report for all users.
System to run for	Enter the system to run the report for. The default is to run the report for the current system.
Number of records to process	Enter a maximum number of records to process.
Open command prompter	Select this to open the Run Query

	dialog where you can add additional filters.

4. Enter your required parameters and click **Finish** to run.
   If you selected the **Open command prompter**, the **Run Query** dialog opens. Click **Advanced** to expand the dialog and access additional filters.
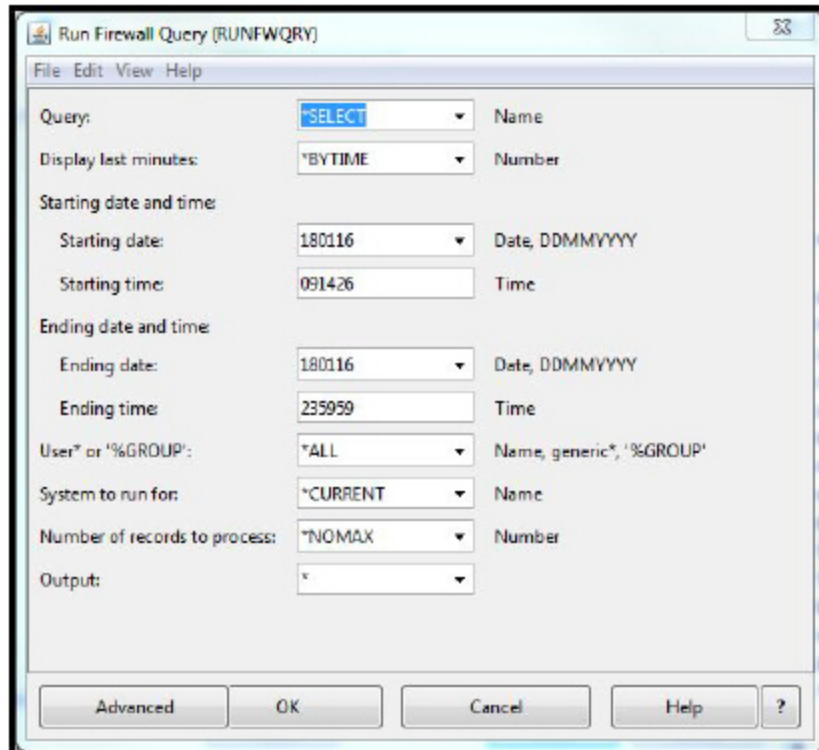
Options/Parameters	Description
Basic parameters	The basic parameters are described in the dialogs above.
Type	Filter the report by Audit Type
Program Name	Filter records by the name of the program that created the journal record.
Job name, user, number	Filter records by the IBM i (OS/400) job name, user, job number.
Filter by time group: Relationship, Time group	Relationship: ***IN** = Include all records in the time group ***OUT** = Include all records not in the time group ***NONE** = Do not use time groups, even if included in the query

	definition ***QRY** = Use time groups as specified in the query definition Time group: **Name** = Name of time group ***SELECT** = Select time group from list at run time
Original command sent from	Filter by the name of the command that created the journal entry
Object	**Name** =Enter the name of the object to be created ***AUTO** = The system will create a name for the object to be created
Directory ('/dir'/')	Enter the directory to contain the created object
User defined data	Internal use only

5. Enter your additional filters and click **OK**. The Query runs and the report is produced.

Schedule Reports

1. Select a report to schedule and click **Schedule**. The **Add/Remove Query from Scheduler** dialog is displayed.
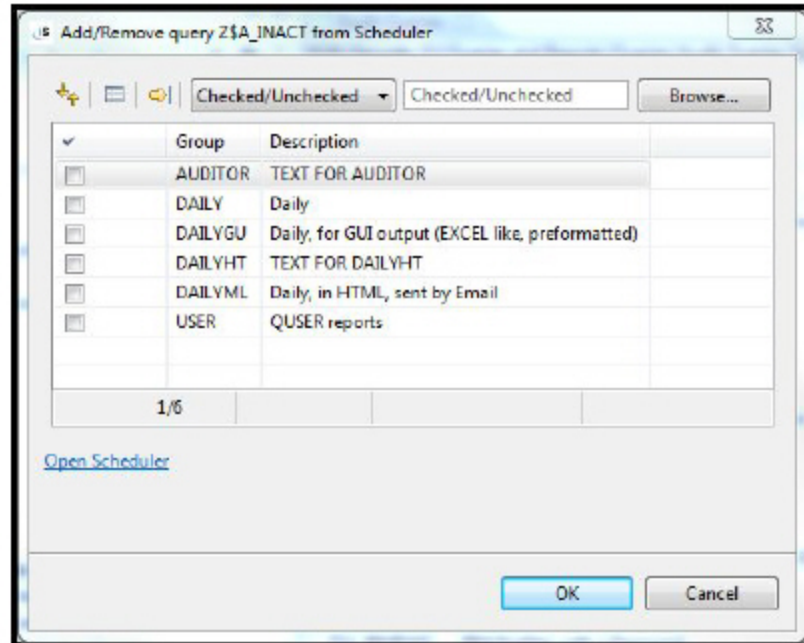
1. 2.Select one or more report groups and click **OK**. The Query is added to the report group.

Edit Reports

This section describes how to edit a query in the GUI. For a full description of the fields and options, please see the appropriate manual.

NOTE: The example given is for an Audit Query, but the procedure is valid for all types of Query.

1. Select a report to edit and click **Open**.
   The **Edit Query** dialog **> General** tab is displayed.
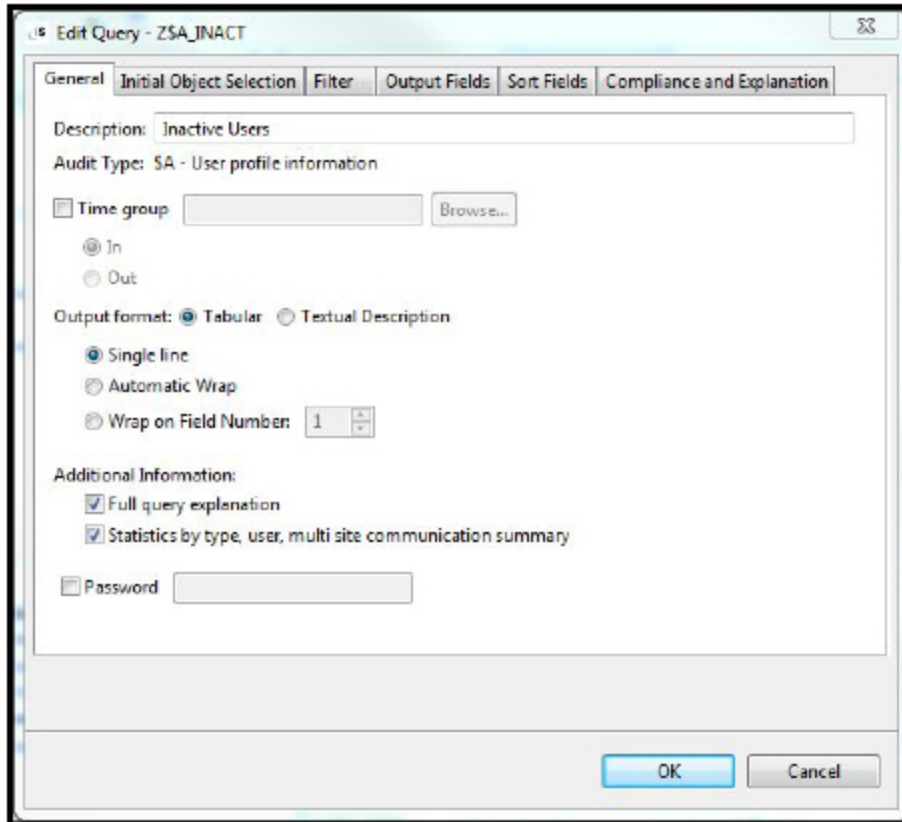
2. Set the general conditions for the output format and displaying header and total.
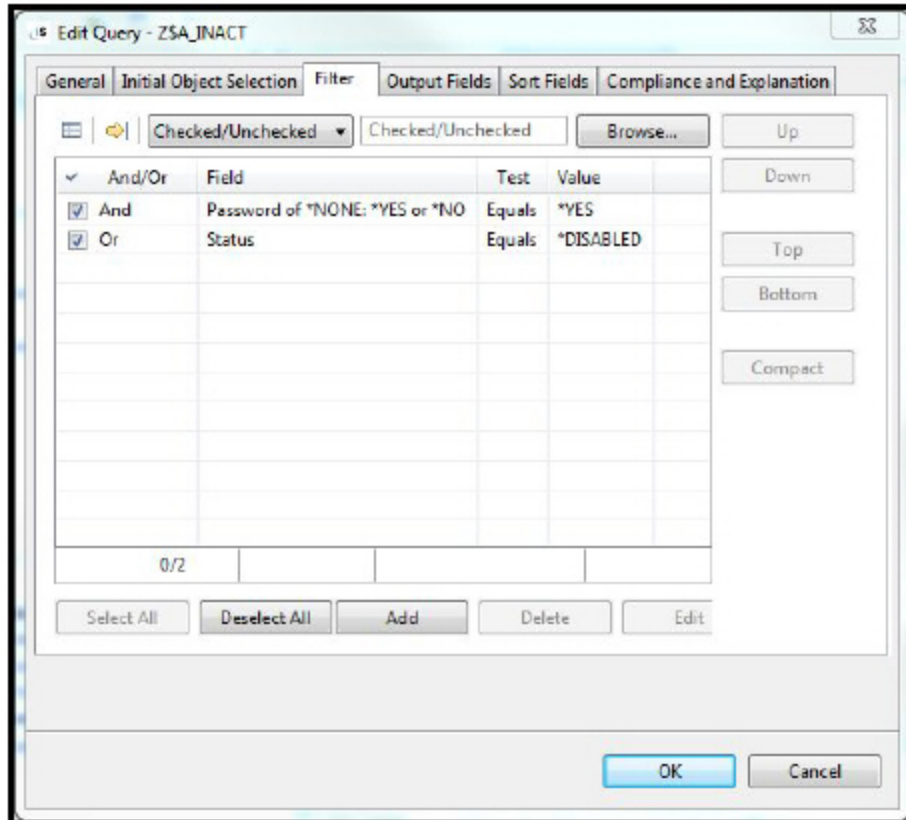
3. When editing the filter, click **Add** to add more filters. The **Add** dialog is displayed.
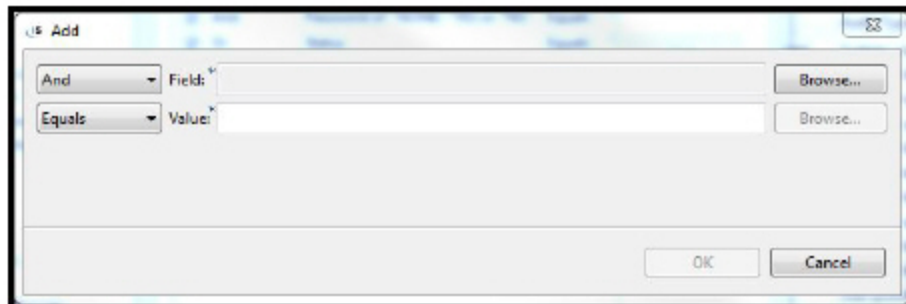
4. Click **Browse** to search for fields. The **Fields** dialog is displayed. The list of shows both generic and file fields. The generic fields are grouped and shown first.
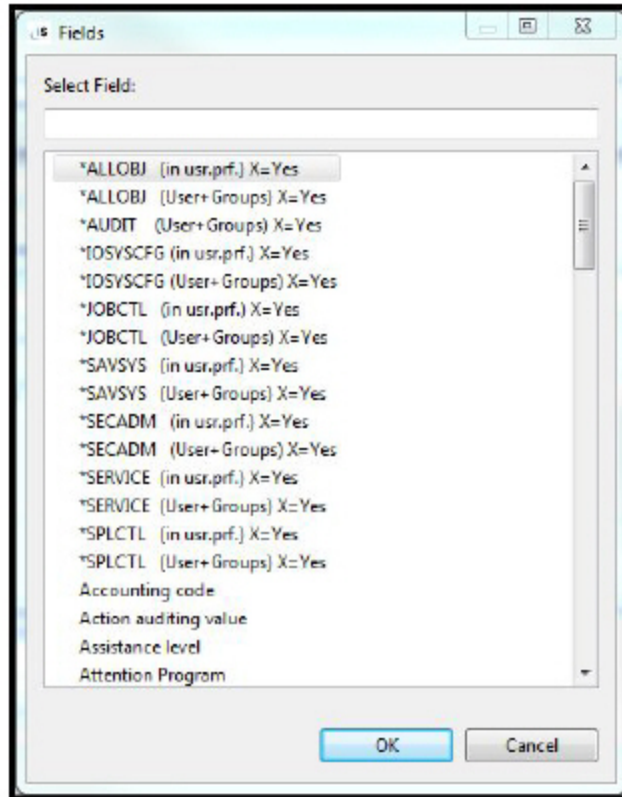
5. Select the Output tab to define the fields that will appear on the report.
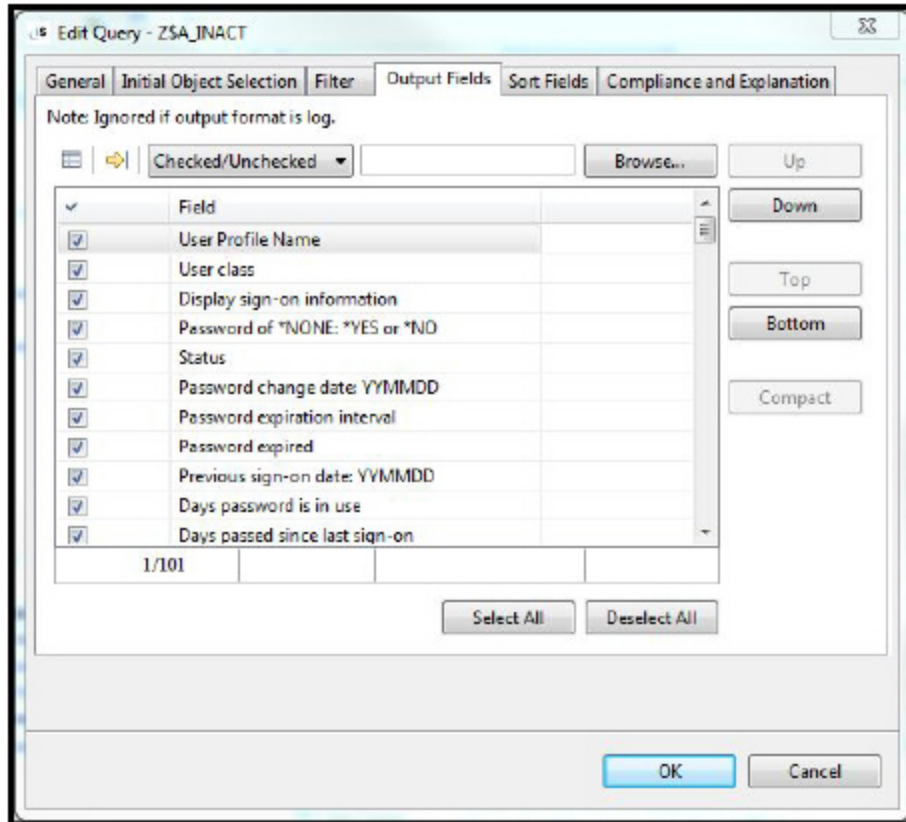
6. Select the **Sort** tab to define the order of the report.
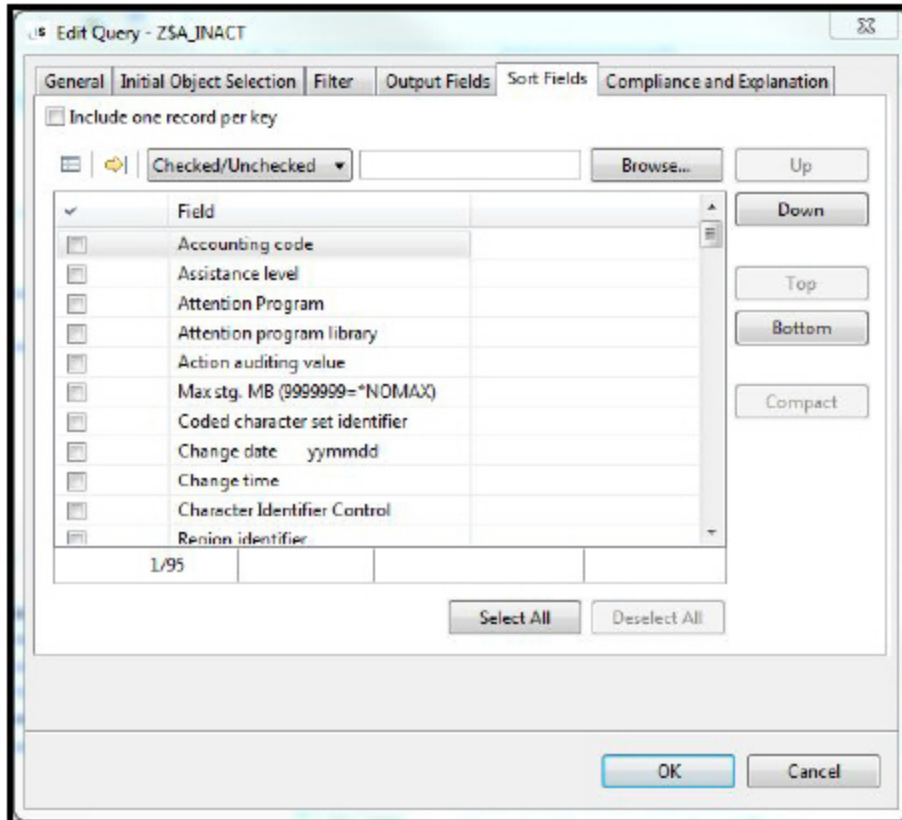
7. Select the **Compliance and Explanation** tab to add information about which compliance requirements are fulfilled by this report and also to give a textual explanation of the report parameters.
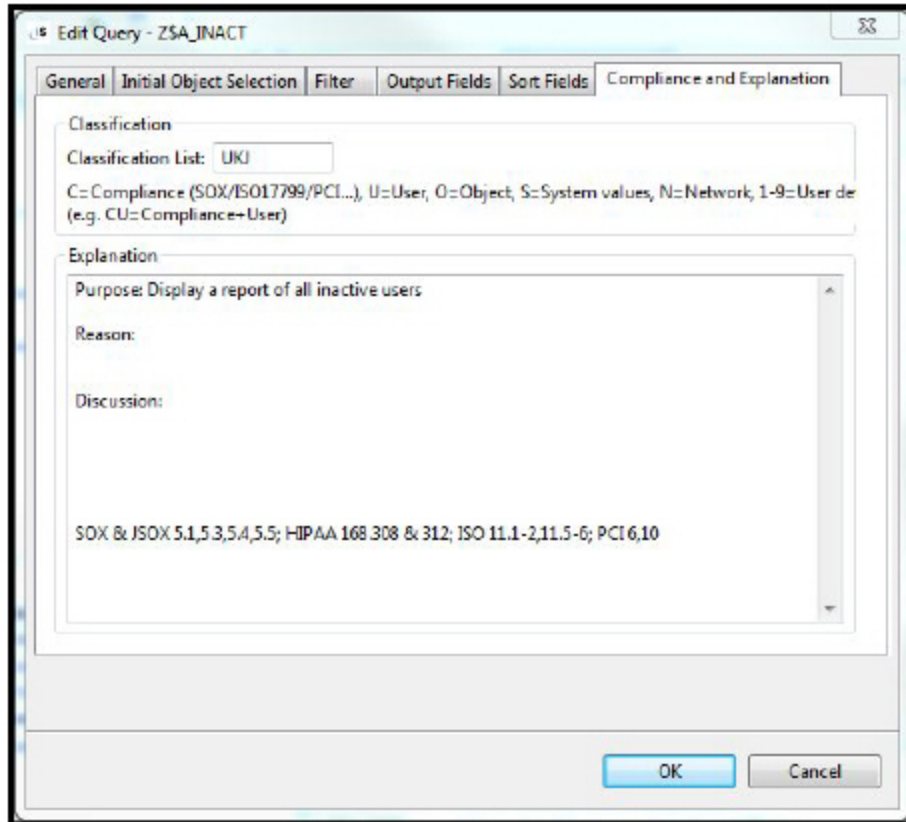
8. When you have finished editing, click **OK**. The updated report is now available.

View Reports

Reports that were generated from the green-screen can be exported and displayed in OpenOffice Spreadsheet. These reports are the result of batch and scheduled query activations sent from the green-screen to an output file.

NOTE: This example describes the procedure from Audit but also applies to Firewall.

1. Select **41. Queries and Reports** in the Audit main menu in the green-screen version.
2. Select **1. Work with Queries** in the **Queries** menu.
3. Select the Query you want to work with and type **5** to run a selected query, or **6** to print it. The **Run Audit Query** screen is displayed.

4. Define the query's parameters and type *OUTFILE at the **Output** field. Press **Enter** to run.
5. Navigate to **Queries and Reports -> Ready Reports** in the GUI. Select **Output Files**. A list dates with available output files is displayed.
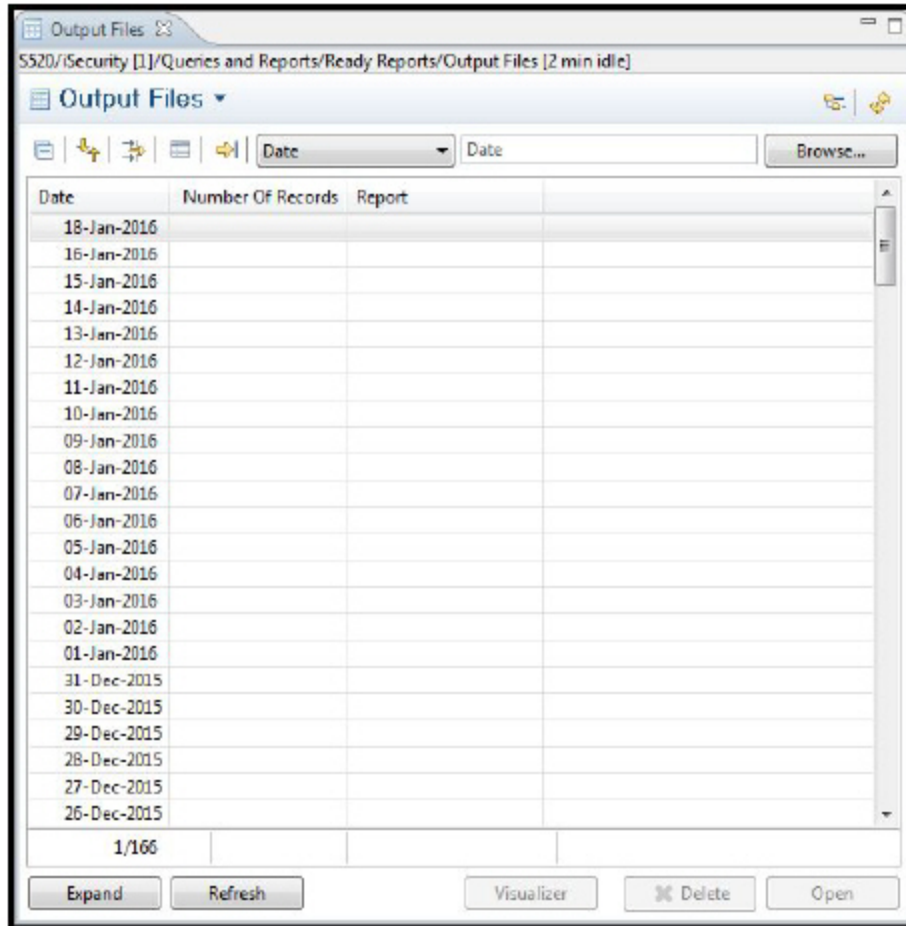
6. Expand the date when the report was run and double click on the specific report. The report opens in a new editor.
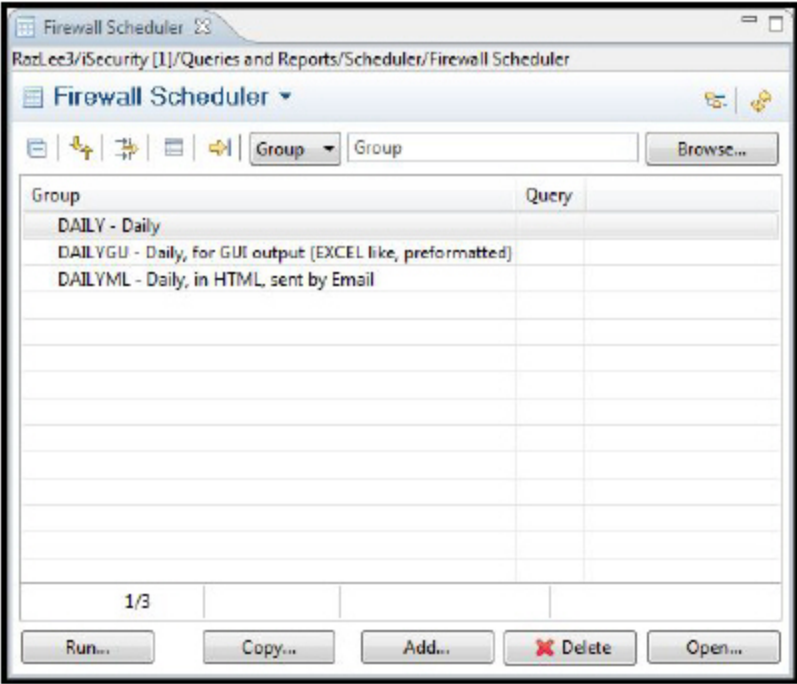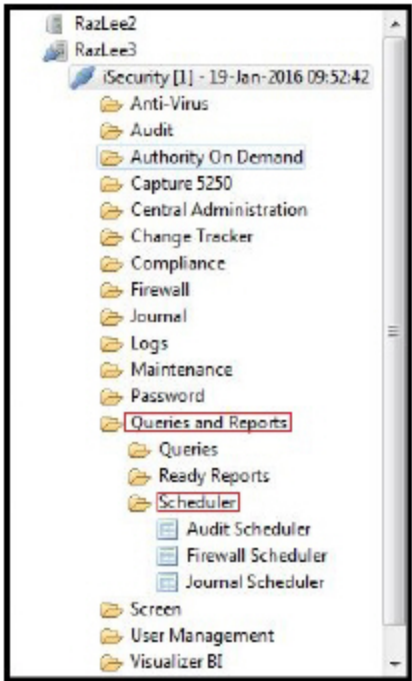
Scheduler

Overview

The **Report Scheduler** allows you to run predefined Report Groups automatically according to a fixed schedule. A Report Group is comprised of one or more individual queries, reports or history log inquiries that are executed together at a designated time. Grouping of reports in this manner is more efficient because the scheduling details and other run-time parameters need only be defined once for the entire group.

The most common application of the **Report Scheduler** is automatically running periodic audit reports based on your queries. You can create a schedule to run reports on a daily, weekly or monthly basis. Additional schedule parameters are provided that allow you to specify the day of the week, day of the month and time of day that your report will run.

Report Schedulers are available for Audit, Firewall and AP-Journal. The examples in this section will use the Firewall Scheduler, but the process is the same for all three products.

To access the Report Scheduler, navigate to **Queries and Reports -> Scheduler**, and double-click the Scheduler you want to work with.
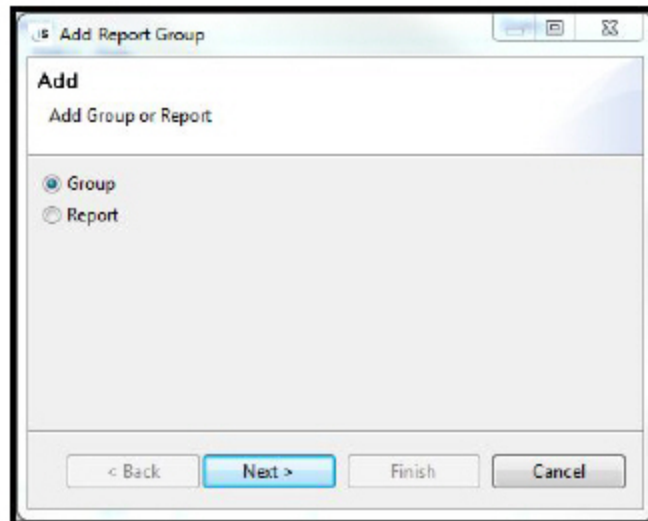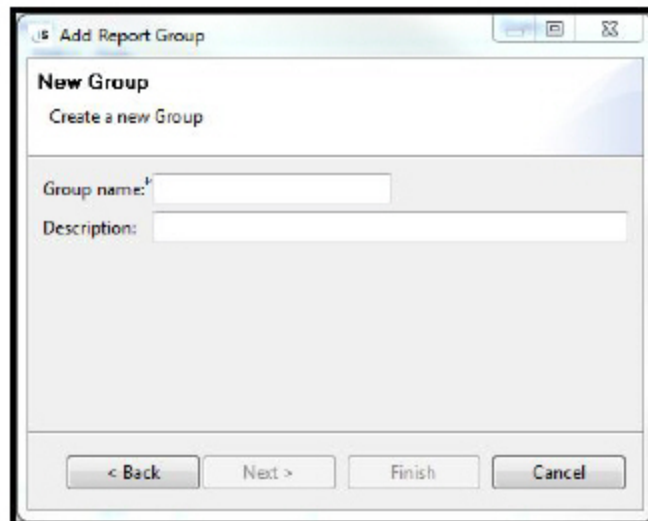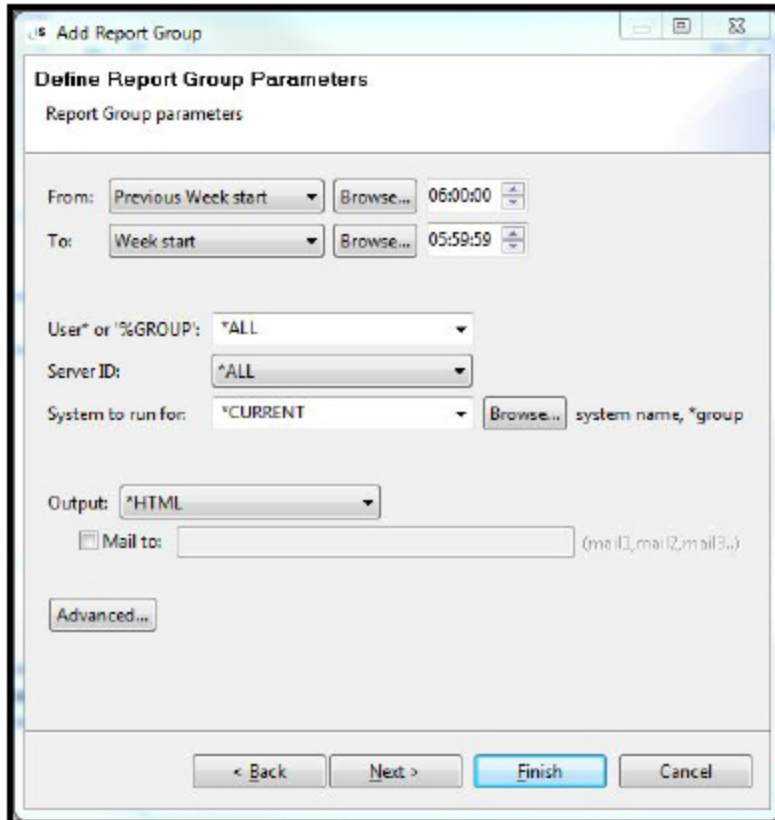
Add a New Scheduler

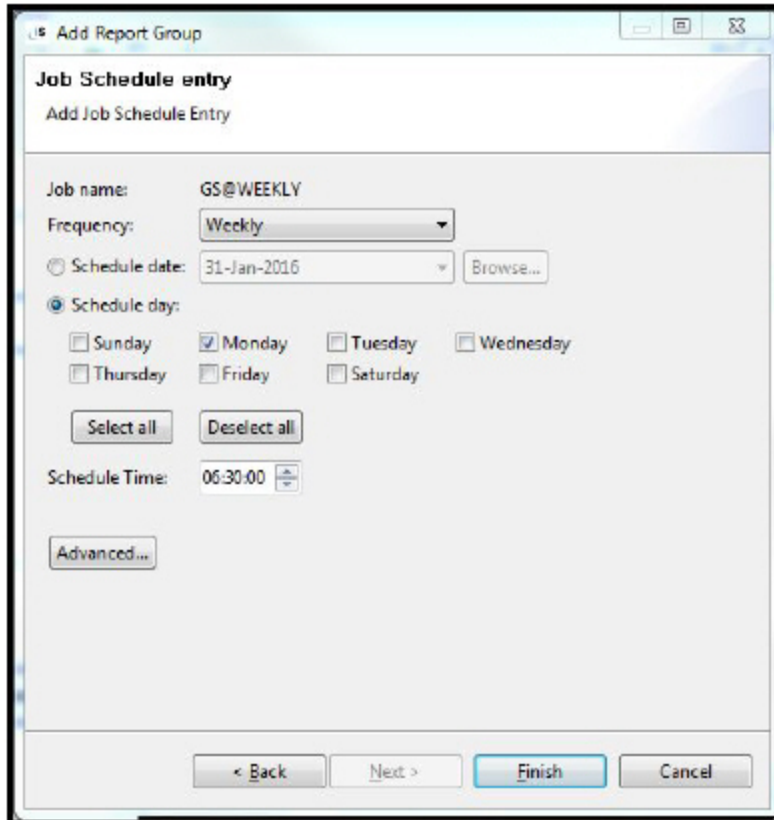1. Click **Add**. The **Add Report Group** dialog is displayed.

2. Select **Group** and click **Next**. The **New Group** dialog is displayed.

3. Type a Group name and a meaningful description and click **Next**. The **Define Report Group Parameters** dialog is displayed.

4. Enter the Report Parameters to define the Time Range, Users, Server, Computer, and Output format.
5. Click the **Advanced** button for more parameters.
6. Click **Next**. The **Job Schedule Entry** dialog is displayed.

7. Define the frequency and time interval of the report.
8. Click the **Advanced** button for more parameters.
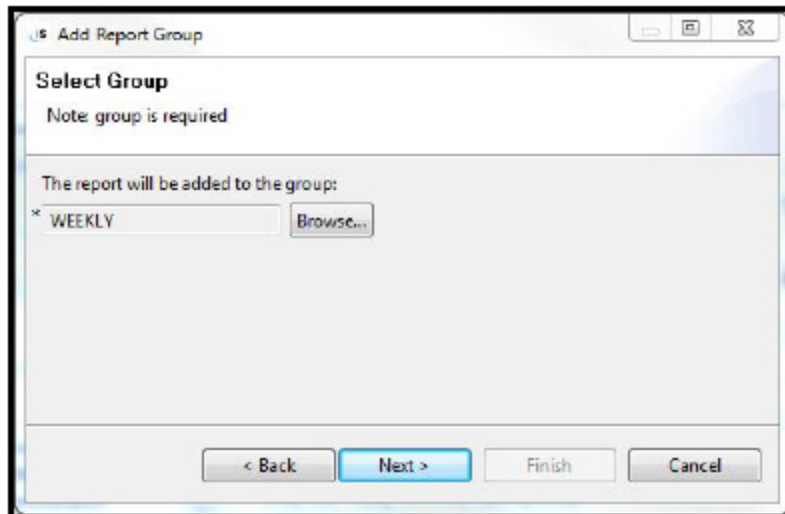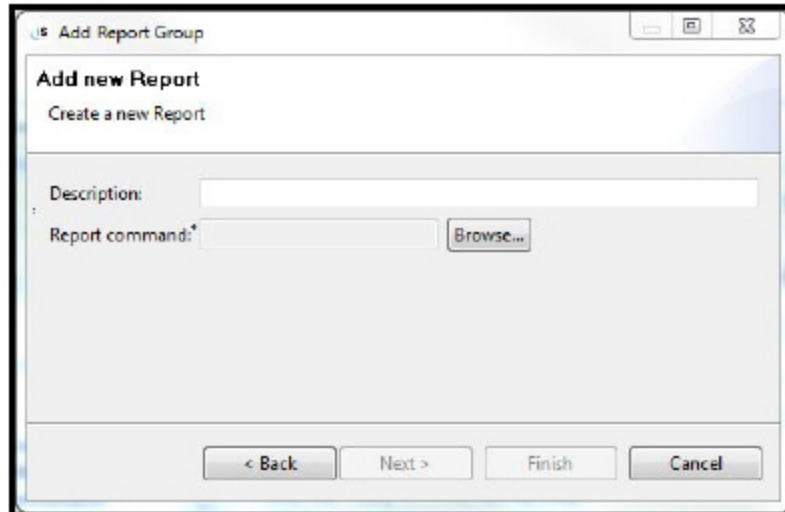9. Click **Finish**. The schedule is now ready to have reports added.

Add Reports

1. Select the group to which you want to add reports and click **Add**. The **Add Report Group** dialog is displayed.
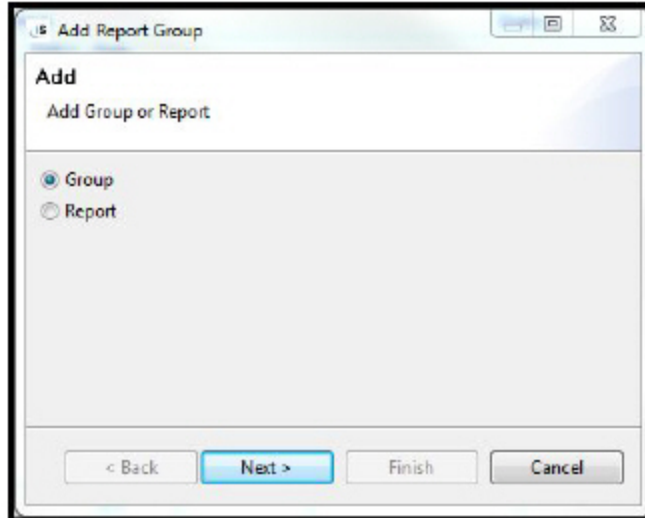

2. Select **Report** and click **Next**. The **Select Group** dialog is displayed with your chosen Report Group already selected.
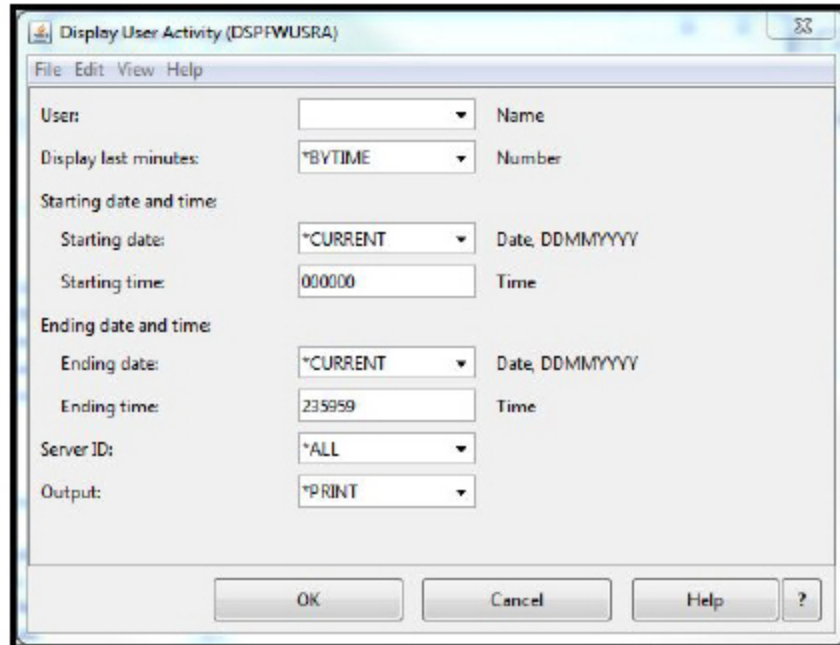

3. Click **Next**. The **Add new report** dialog is displayed.

4. Click **Browse** to select a report. If the report has a description, it will appear in the Description field. If not, enter a meaningful description.
5. Click **Next**. The **Command Parameters** dialog is displayed.
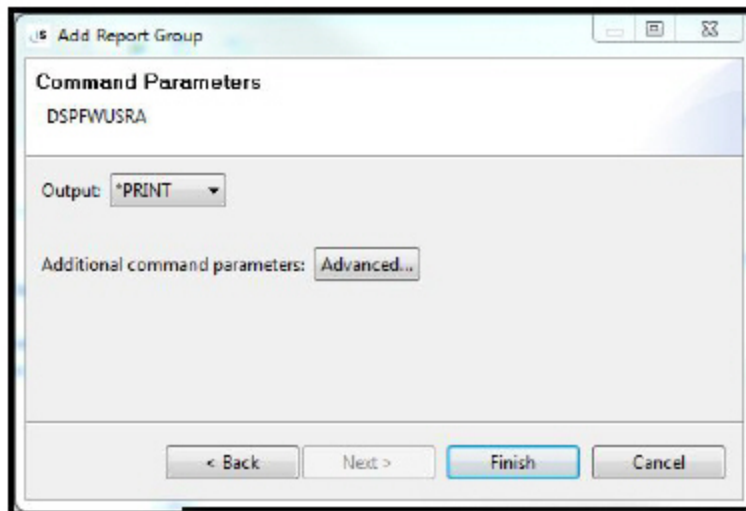
6. Select the Output and Click **Advanced** to set additional parameters for the scheduled report.

-

NOTE: For a description of the parameters, see the appropriate User Guide.

7. Define the additional parameters and click **OK**.
    NOTE: If you do not enter obligatory fields, you receive an error message.

8. Click **Finish** in the **Command Parameters** dialog. The report is added to the schedule.
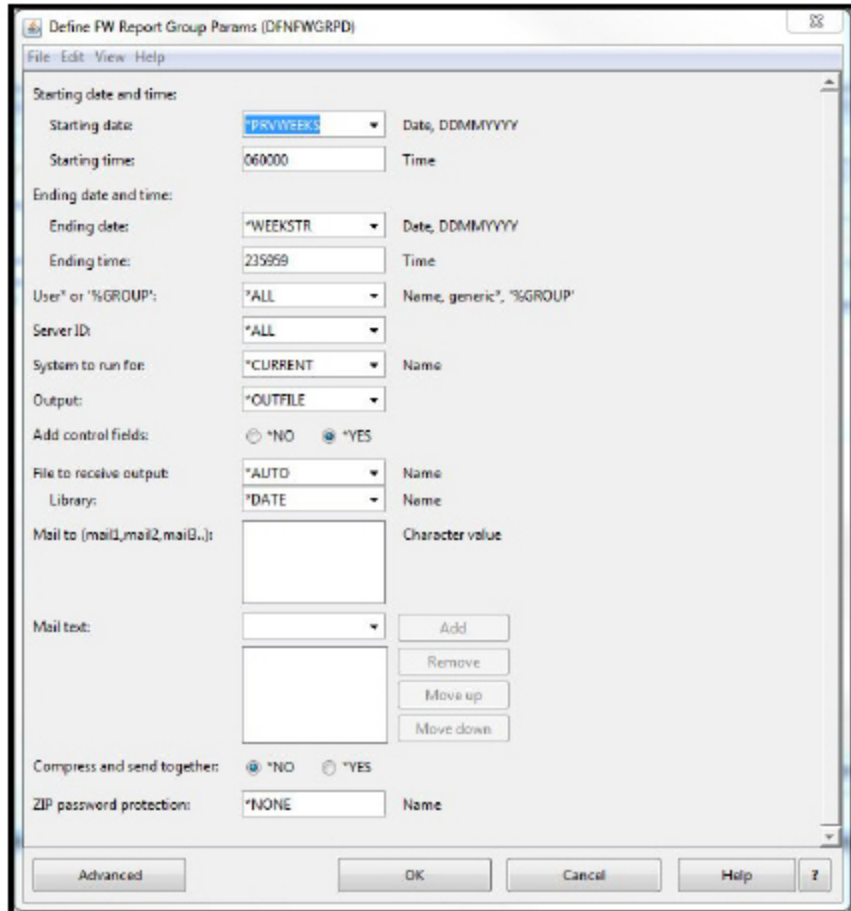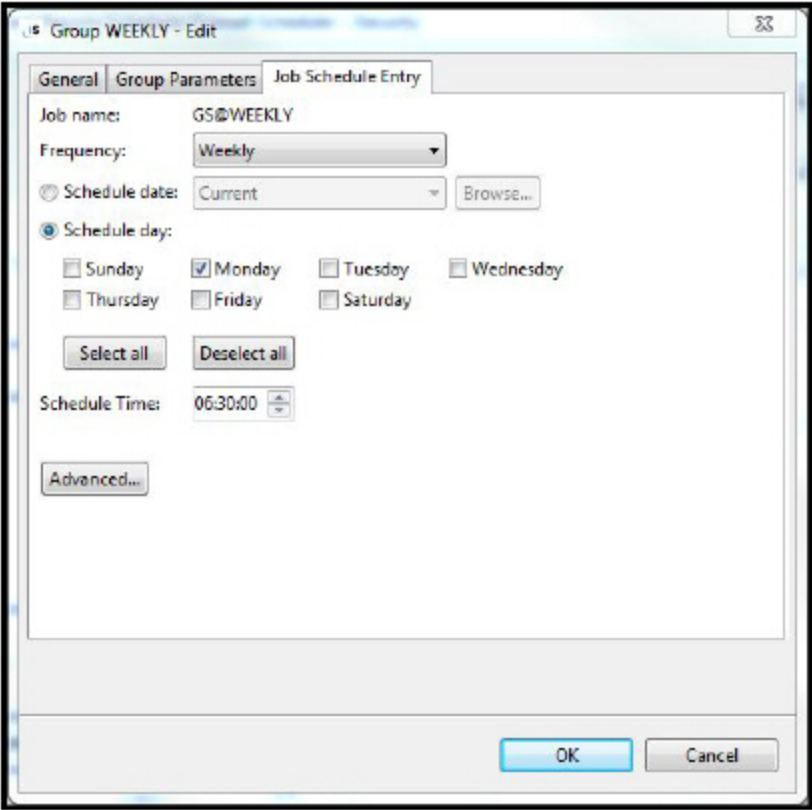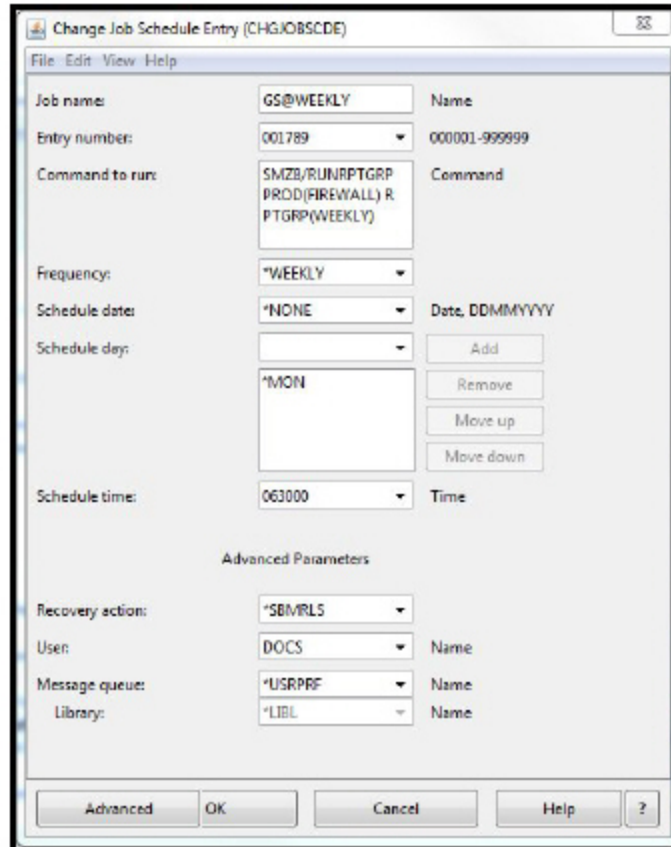
Edit a Group

1. Select the group which you want to edit and click **Open**.
   The **Group Edit** dialog **> General** tab is displayed.
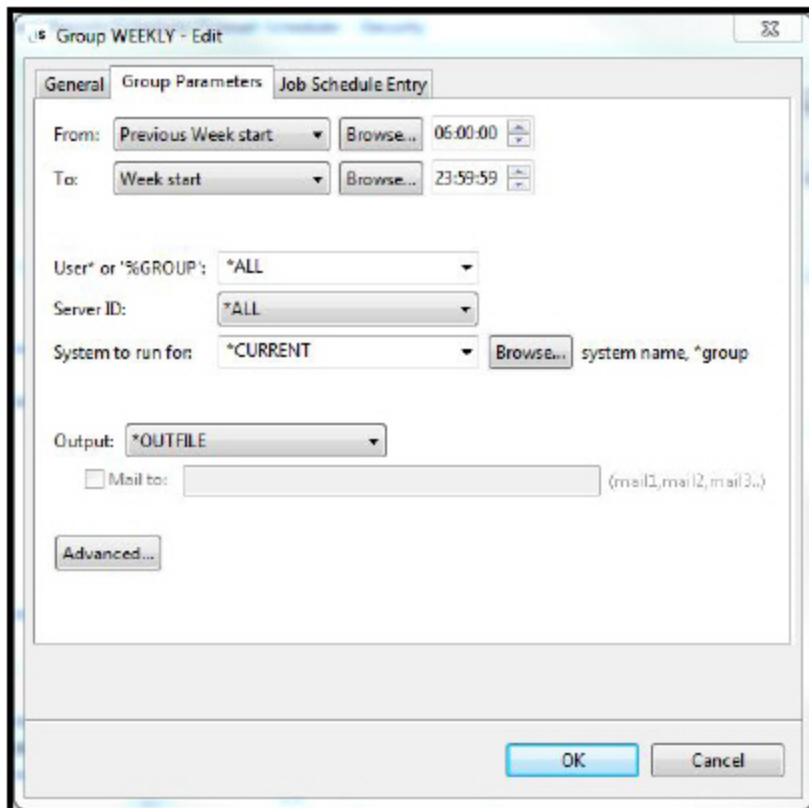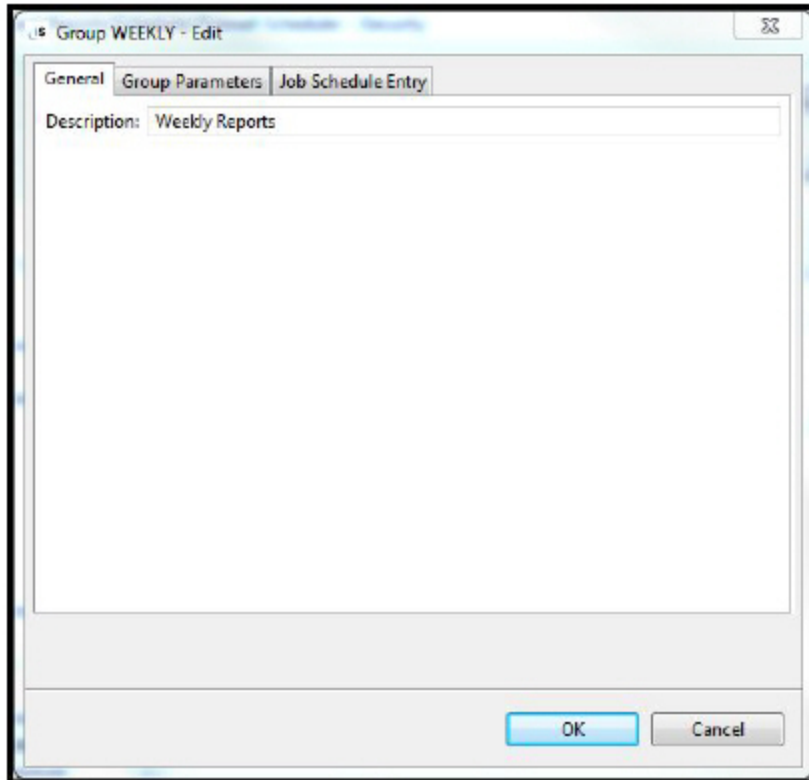
2. Use the three tabs to edit the group definitions. Both the **Group Parameters** and **Job Schedule Entry** tabs have an **Advanced** option, which opens additional parameters.

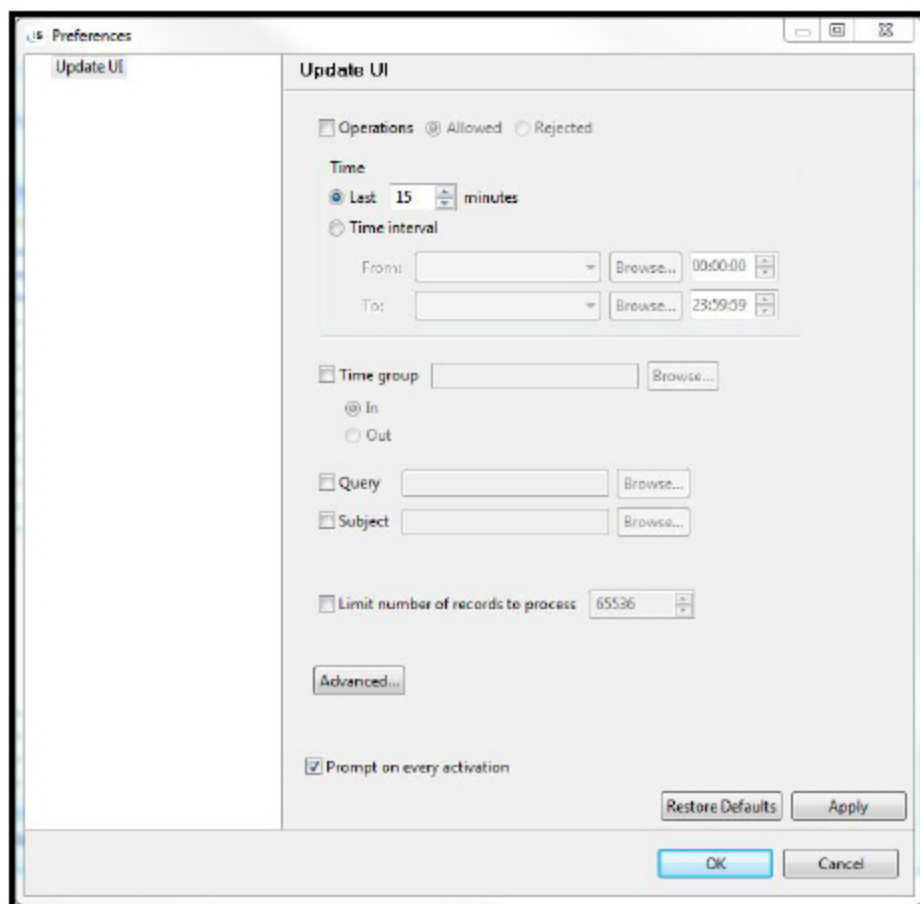3. Click **OK**. The Group definitions are updated.

Logs

Activity Log

This feature is useful not only for standard report analysis but also for investigating immediate problems such as program failures, errors or suspicious activity. Firewall, Audit, Action, and Password includes many ready-to-use log display parameters. Press **Enter** and the specified data appears in seconds. You can also choose to print a hard copy of the Activity Log results. To use the Activity Log, follow this procedure.

The following example is based on Firewall but is relevant for all modules

1. Navigate to **Logs -> Firewall** and click **Firewall Log**. A Filter screen is displayed.

Options/Parameters	Description
Operations	**All** = Show all log messages **Reject** = Show only reject messages **Allow** = Show only allow messages
Time	**Display last n minutes** = This Backward Glance feature lets you look at the last several minutes of activity without the need to define specific time or date parameters. Just enter how long a period (in minutes) you wish to look at, click Enter, and transactions occurring during that period of time quickly appear. Backward Glance really comes in handy when assisting users with those nasty error messages that pop up verifying that a batch job has successfully completed. Enter the desired number of minutes **Display time interval** = Selects only those events occurring within the range specified by the starting and ending date/time combination.
Filter by time group	The Activity Log displays make full use of the convenient time group feature. This time-saving feature further enhances your ability to reach your critical data quickly. **Relationship:** **None** = Do not use time group, even if included in query definition **Out** = Include all records not in time group (Exclusive)

-

	In = Include all records in time group (Inclusive)
Query	Use an existing query to filter Activity Log entries. This is useful for applying complex filter criteria. **Name** = Name of an existing query ***None** = Do not use query rules (Default)
Maximum Numbers of Records	***NOMAX** = No maximum (Default)

2. Select your parameters and click **OK**. The Log is displayed.
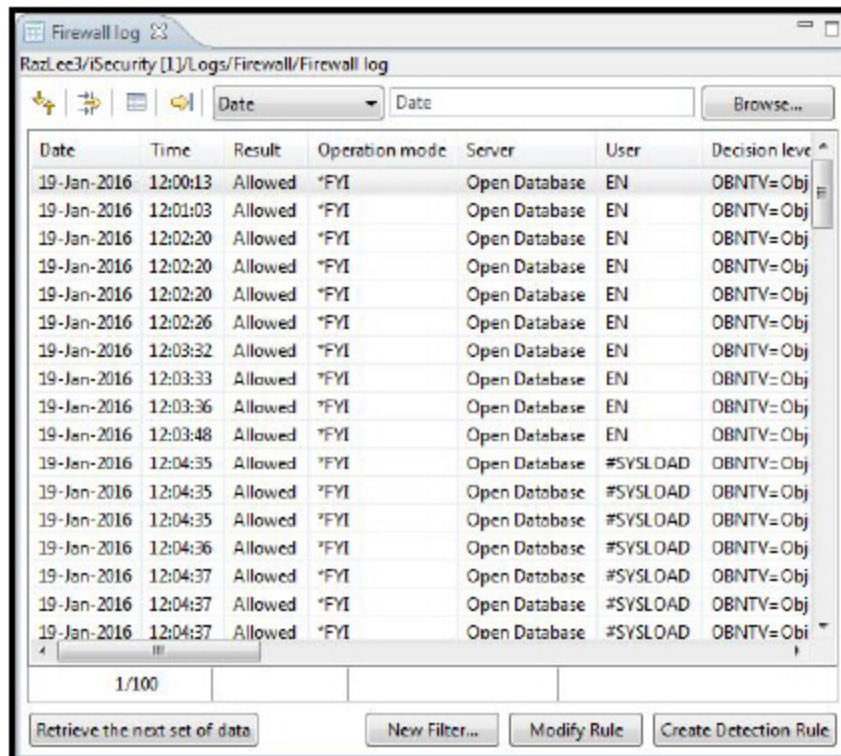
3. Click **Retrieve the next set of data** to display the next 100 transactions.
4. Double-click a row to view the full log information.
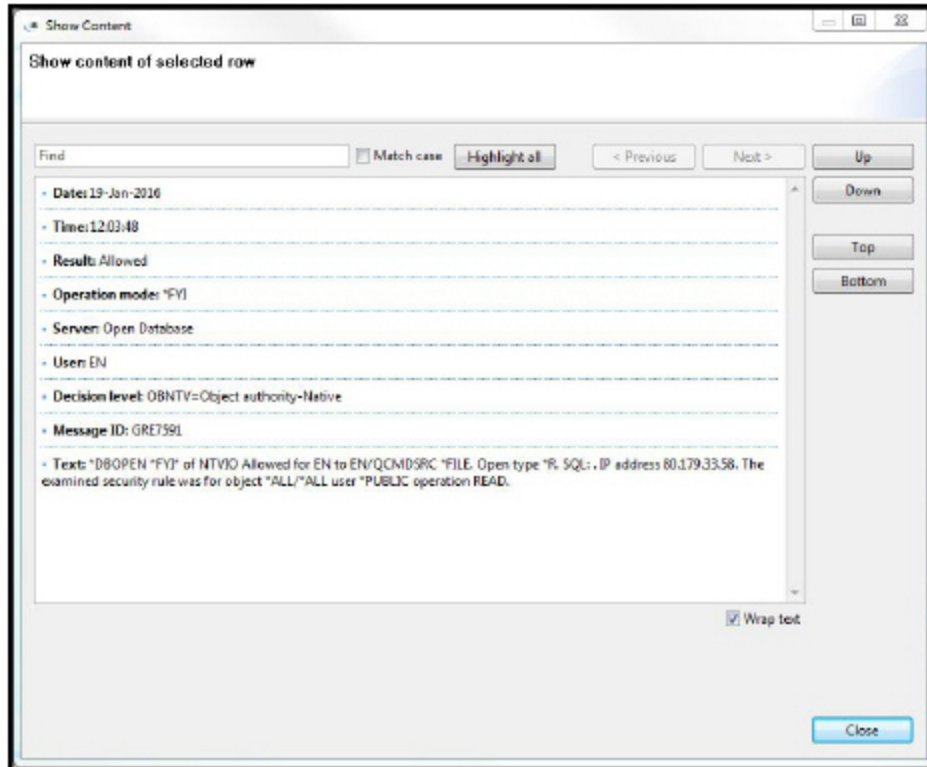
You can use **Up**, **Down**, **Top**, and **Bottom** to scroll within the log.

You can Select a log transaction and click **Modify Rule** to change a rule's definitions. You can select a log transaction and click **Create Detection Rule** to add a new real time detection rule.

Export as CSV

This option allows you to save your Activity Logs in your computer in a CSV format. CSV Files (comma separated value files) are a standard format for transferring data between databases or spreadsheets (such as Microsoft Excel). CSV Files are ASCII encoded and so can be edited in any Text Editor.

To export Firewall logs to CSV format:

1. Navigate to **Logs -> Firewall** and click **Export as CSV**. The **Filter** dialog is displayed.
2. Set your parameters and click **OK**. Your PC opens a dialog where you can specify the directory to which to save the file and the name for the file.
3. Navigate to the required directory, enter a name and click **Save**. Your log is now saved in CSV format.

Export Spreadsheet

This option allows you to save your Activity Logs in your computer in Excel, OpenOffice spreadsheet, HTML or PDF formats.

To export Firewall logs to a spreadsheet:

1. Navigate to **Logs -> Firewall** and click **Export**. The **Filter** dialog is displayed.
2. Choose your export format, set your parameters and click **OK**. Your PC opens a dialog where you can specify the directory to which to save the file and the name for the file.
3. Navigate to the required directory, enter a name and click **Save**. Your log is now saved in a spreadsheet format.

-

Visualizer BI

Overview

Visualizer BI is an advanced data warehouse solution that allows IT managers to graphically analyze security-related system activity quickly and easily.

Visualizer BI uses business intelligence techniques to process large quantities of transaction data with minimal storage requirements. This process eliminates the need for time-consuming log scanning and tracking activities that tie up system resources and increase IT operating costs.

Most security analysis products pose a problem for system administrators who face a "needle in a haystack" when searching a task, security breaches or other critical system activity. Visualizer BI makes the whole process painless, simple, and cost-effective.

Visualizer BI presents the user with a user-friendly, JAVA-based GUI, simplifying the whole process even for technologically-challenged users. The user simply points, clicks, and drags the appropriate parameters to the filter section of the GUI where a pie chart is displayed in seconds with all the relevant information. To tweak the analysis use the mouse to make the few changes and the revised results are displayed.

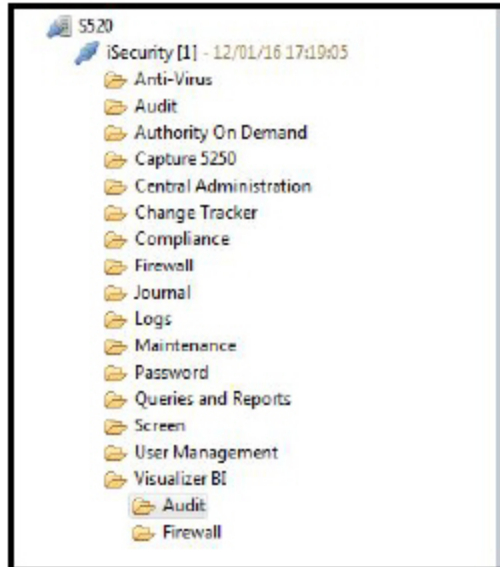Visualizer BI is available in versions that work with Firewall, Audit and AP-Journal.
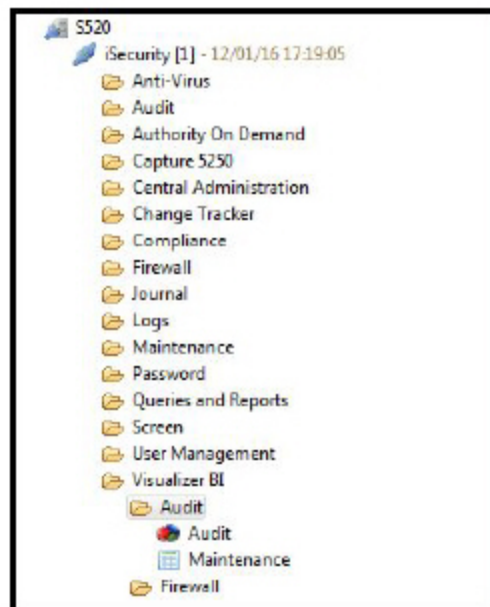
Working with Visualizer BI

This example is based on Visualizer BI for Audit.

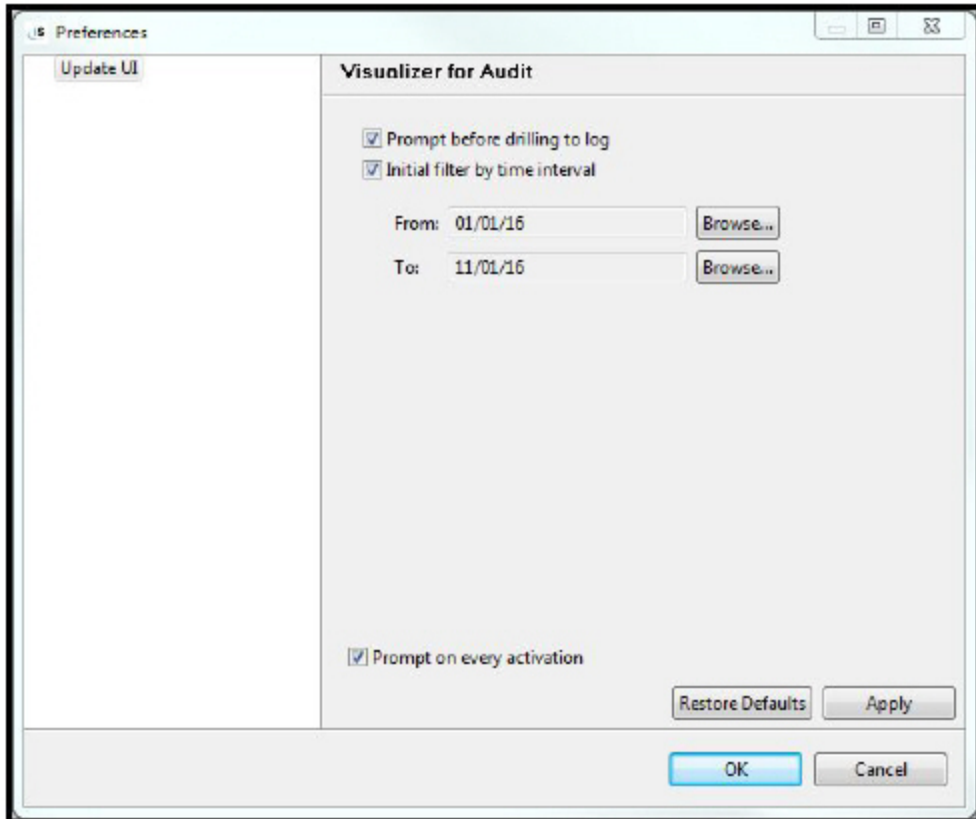To open and begin working with Visualizer BI:

1. Double-click the **Visualizer BI** node to open the navigation tree.


2. Double-click the **Audit** node.

3. Double-click **Audit**. The initial filter dialog is displayed.

Parameter	Description
Prompt before drilling to log	Select this if you want to add additional time filters before drilling to the actual data.
Initial filter by time interval	Select this to enable an initial filter by date. If you do not filter by date, data for the complete file will be displayed.
From	The date for which to start extracting data. The default date is 10 days before the **To** date. For example, if the **To** date is January 16th, the **From** date is January 6th.
To	The date for which to finish extracting data. The default date is the last date for which there is information (usually today).

|	
Restore Defaults	Click **Restore Defaults** to restore the original extract parameters.
Apply	Click **Apply** to save your extract parameters without running the report. The next time you open Visualizer BI, these are the parameters you will see.

4. Click **OK**. The initial Visualizer screen is displayed.
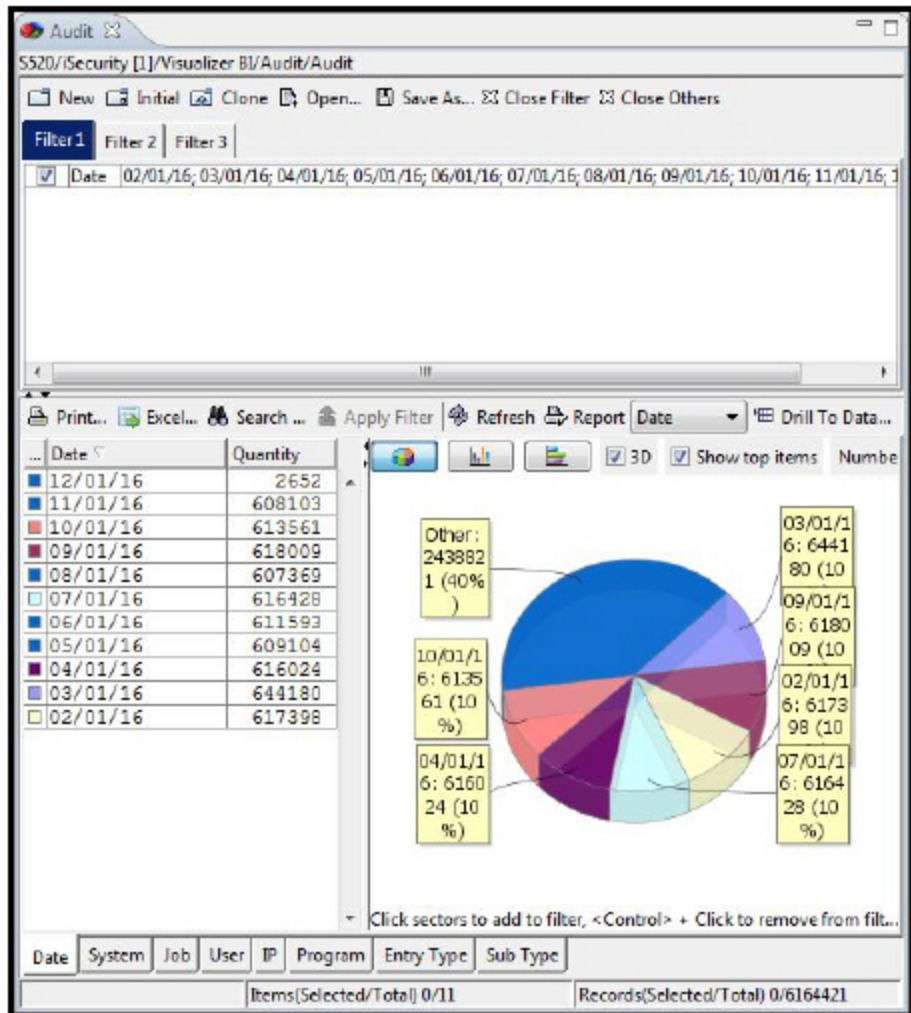
NOTE: In order to work with Visualizer BI for AP-Journal, navigate to **Journal -> Application Outputs**, select the required application, and click **Visualizer**.

The Visualizer BI Interface

The following screen-shot is the main interface window for Visualizer BI, the graphic-analysis security component of iSecurity. The table describes the main components.
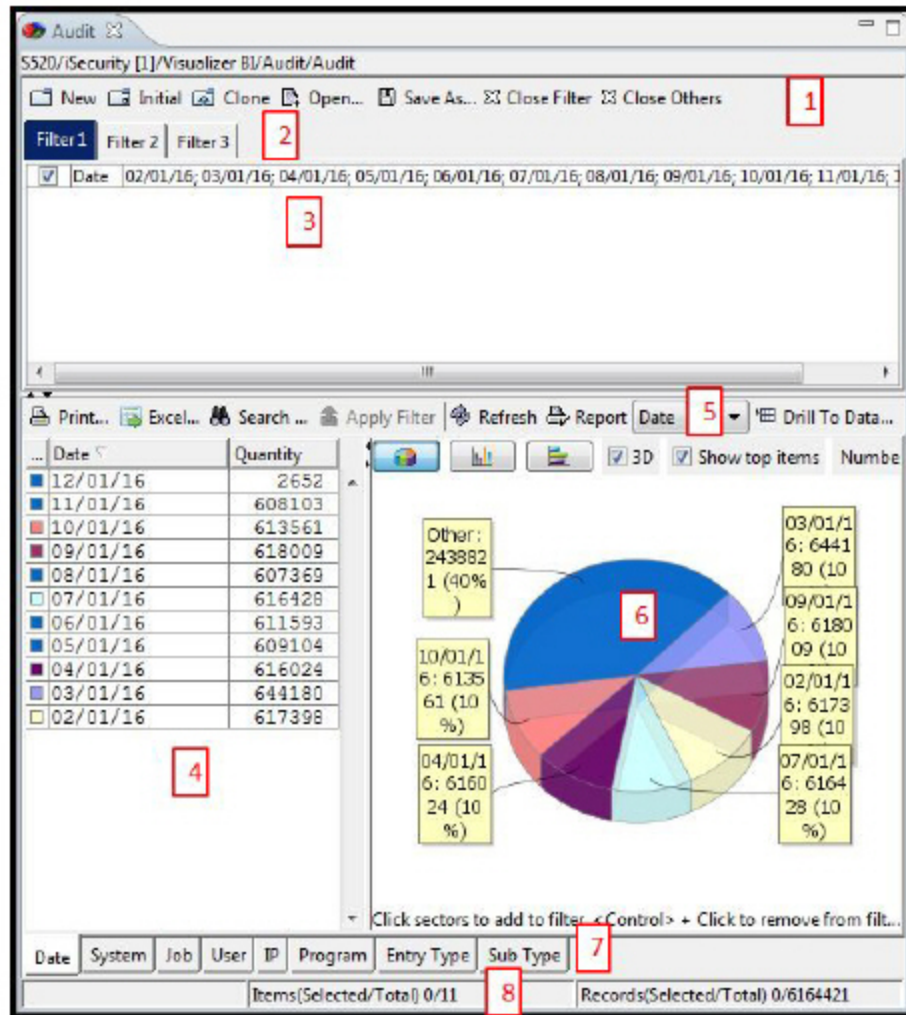
Number	Name	Description
1	Toolbars	The toolbar allows you to perform basic navigation tasks. ![] **New** = Creates and opens a new filter tab ![] **Open** = Opens a previously-saved filter

		🖫 **Save as** = Allows you to save filter data 🗑 **Remove** = Delete a filter 🖨 **Report** = Generates an HTM report
2	Filter Tabs	Allow you to navigate between open filters
3	Filter Pane	Area where filters are displayed
4	Data Pane Toolbars	Tool-bar that allows you to work with the Data Pane
5	Data Pane	Area where Dimension data is displayed. 🖨 **Print Table** = Print data 📄 **Excel** = Export data to spreadsheet 🔍 **Search** = Search and add to the filter 🏛 **Apply Filter** = Click to apply selection to the filter. 🔄 **Refresh** = Click **Refresh** after the fetch size has been modified. 🗔 **Drill Down**= Filter by specific time and limit number of records to process.
6	Pie Chart	The pie-shaped representation of your security and system data. You can also display the data in vertical and horizontal bar charts.
7	Dimensions	These criteria enable you to choose how you want to sort and display your data. **Date** = Sorts system activity according to date

-

|		
		System = Select the system with which you want to work **User** = Sorts system activity according to user **Server** = Sorts system activity according to server **Function** = Sorts system activity according to function, such as OPEN, DELETE, and so on **IP** = Sorts system activity according to **IP address** **Library** = Sorts system activity according to library **Object** = Sorts system activity according to object **Result** = Sorts system activity according to Allow or Reject
8	Status Bar	The Status Bar, displays the number of members (units of information-each displayed on a different line) selected, out of total members and the number of entries (to the system) selected, out of total number of entries.

Generating Graphic Reports

NOTE: Visualizer works with a statistical file installed on your system. Therefore, all dates listed in the **Date** dimensions (the default opening setting) in the **Data** pane will be from when the first entries were made to your system.

1. Phrase the data you want to display in this form: (examples). This is known as a **Visualizer BI query.**
   - Date **according to** user (a particular user's entries covering all dates)
   - Server **according to** function (a particular function's entries broken down into a list of the different servers that performed that function)
   - Result **according to** IP (an IP address listed by how many entries were allowed/rejected)
2. Make sure the **Filter** pane is empty, then click the **Dimension** tab of the second part of the Visualizer BI query.
3. Find the specific data in the list and select it. Note that the **Filter** pane immediately displays this information.
4. Click the **Dimension** tab of the first part of the Visualizer BI query. Your query is displayed in the **Data** pane.

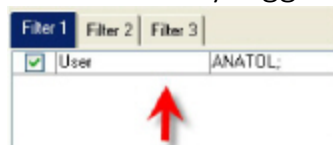The first example listed, date according to user, is shown this way.

1. Click the **User** Dimension tab.
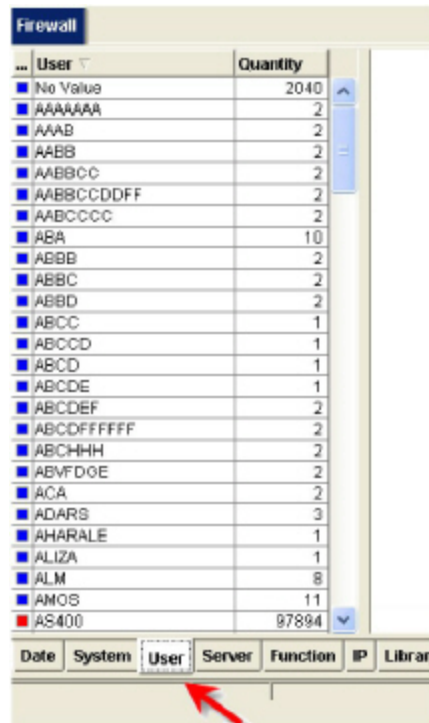
2. Select the user you want to learn about.
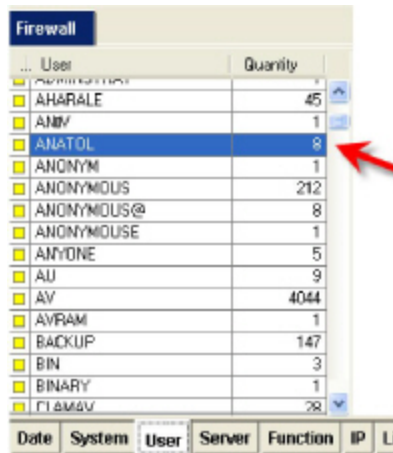
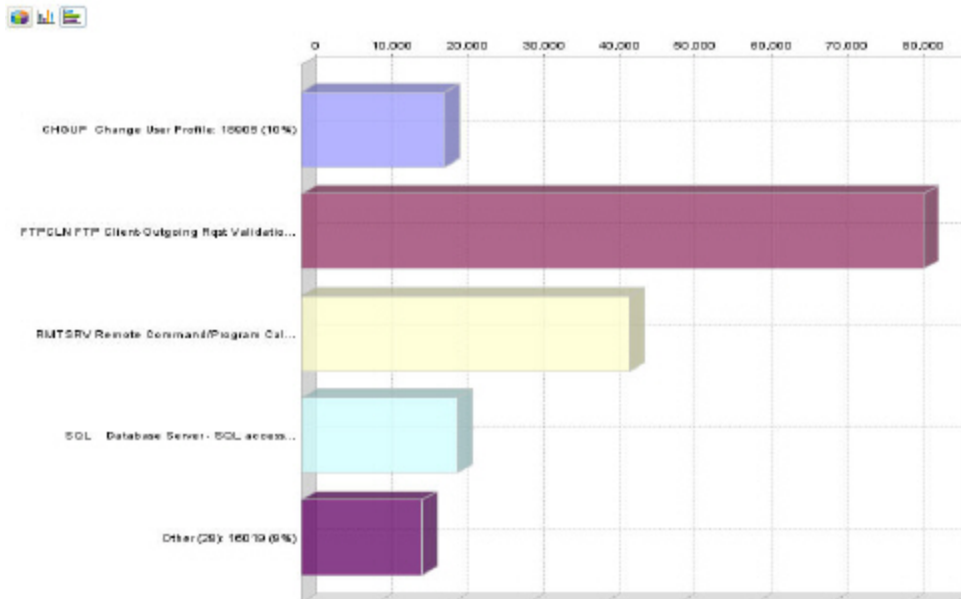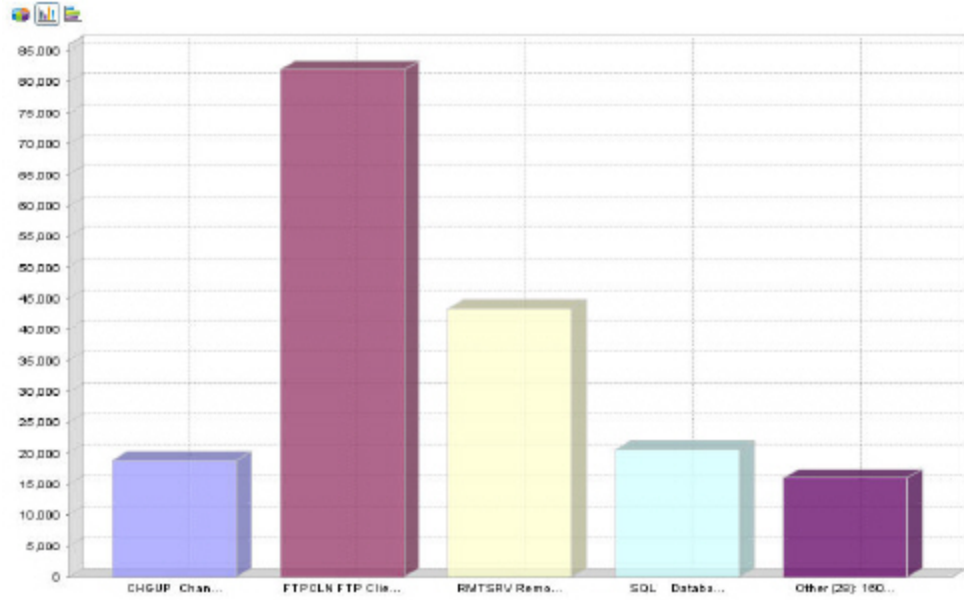3. Note that this selection is immediately logged in the **Filter** pane.

4. Click the tab of the first part of the Visualizer query (in this case, **Date**).
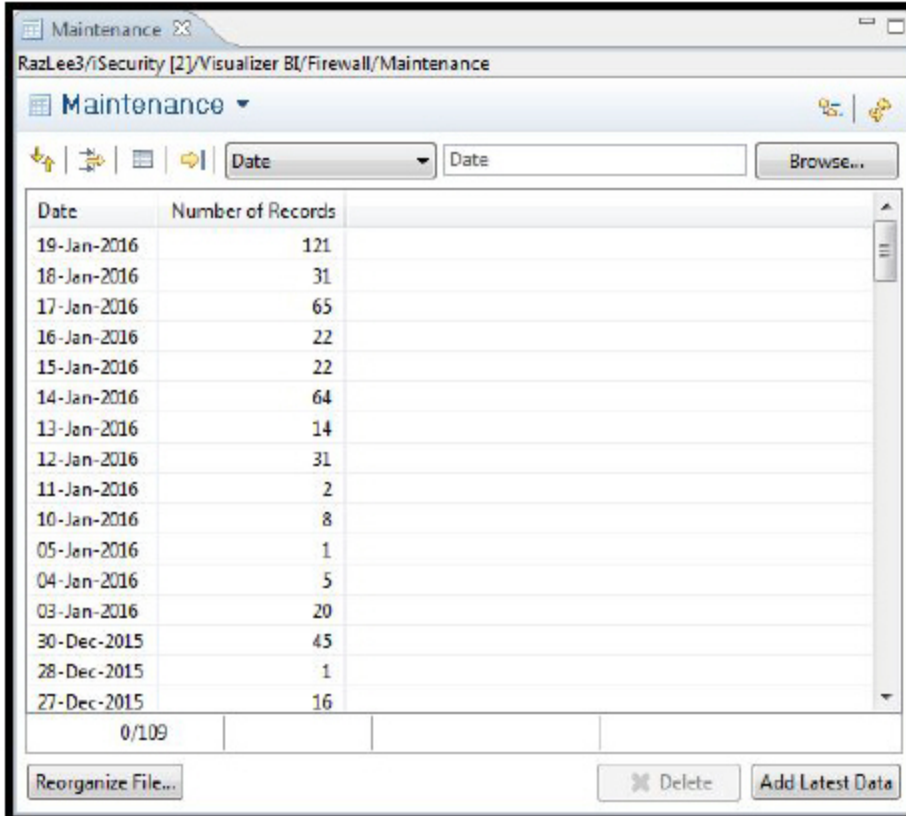
The dates are listed in the **Data** pane immediately or after a few seconds. Next to the date is the number of entries that the user made on each of those dates; the appropriate pie chart is also displayed.
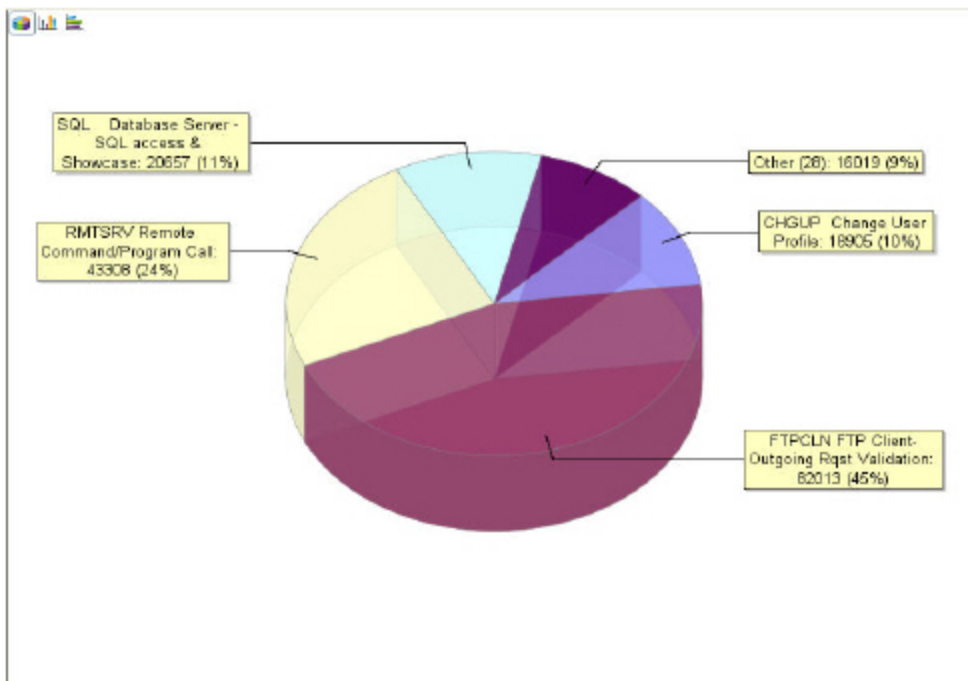
Maintaining the Visualizer BI Data

To maintain the Visualizer, navigate to **Visualizer BI -> Firewall ->**
Maintenance. The **Maintenance** table is displayed.

Add Latest Data

Data is added to the Visualizer statistical files every night in daily maintenance jobs that run on the IBM i (AS/400). Sometimes there is a need to see the most up to date data, so you must manually add this data to the file. To do this, click **Add Latest Data**. You will see a progress bar while the file is being updated and then the new records are displayed in the table.

Delete Entries

The jobs that add data to the statistical files for Visualizer do not remove any records. If you do not manually remove the records, you will have data available from the very first day that you started working with iSecurity.

1. Select the dates you want to remove from the file.
2. Click **Delete**. A **Delete** dialog is displayed which asks for confirmation.
3. Click **Yes**. The records are removed from the file.

NOTE: If you do not delete all records in a given date range, then the results you see in Visualizer will give an inaccurate picture. For example, if you delete the record for October 6th and October 17th in a given year, then any use of Visualizer that includes the month of October for that year will give incorrect information.

Reorganize the File

Reorganizing a file both compresses and reorganizes the physical file in the database. The process places the physical records of the file in the same order as the file index, which reduces file processing time. Reorganizing a file can be a long process. You can choose to run the process immediately or to schedule it for a time when there will be less impact on the system.

1. Click **Reorganize File…** The **Reorganize File** dialog is displayed.
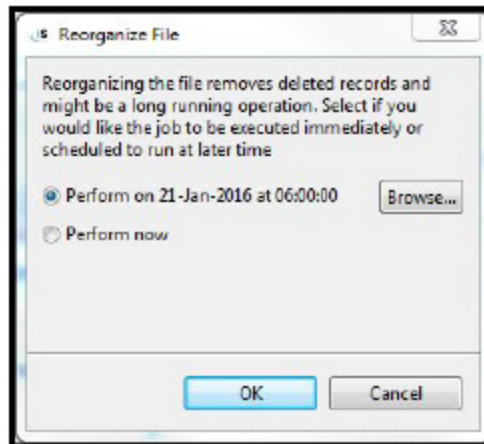
2. Select **Perform now** to run the file reorganization immediately or click **Browse** to choose a date and time to run the reorganization.
3. Click **OK**. The reorganization runs according to your choice.

NOTE: The reorganization of the file can be a long process. While the process is running, Visualizer BI is not available. You should make sure to schedule the reorganization at a time when the process will have the least impact on your system.