helpsystems

User Guide
Viewpoint Administrator

Copyright Terms and Conditions

Table of Contents

Welcome to Viewpoint Administrator

Viewpoint Administrator provides a single point of access to functions previously available only from a 'green screen' terminal or 5250 emulation session. Administrator should not be installed for every Viewpoint user. Install only for those that will manage the following functions:

Set Defaults

Easily manage Sequel user defaults for individuals or groups. Create defaults for new users from pre-built default templates.

Host Auditing

The Auditing module lets you keep track of the host and Viewpoint requests that are run on your system. In short, Auditing provides a way to monitor your investment in Sequel.

Database Security

Add another layer of security to your database. The Inclusion / Exclusion Dictionary supplements system object authority to restrict access to database files and fields.

Advanced Database Security

Administrators can now add advanced levels of database security--in particular, row-level secuity.

Manage Viewpoint Jobs

Obtain a list of current Viewpoint jobs. Review job logs and end jobs if needed.

Active Users

Generate a quick list of active Sequel users and job status.

Manage the Query Option File

Manage current options or add new options to the Query Option File.

Maintain Host Servers

Maintain the Host Servers file for connections to remote databases. Requires V5R2.

SQL Join Data Base

Maintain the file that tracks join fields between iSeries data files for use with the Viewpoint Autojoin feature.

Drill Down Options

Maintain the Drill Down Application option file containing instructions to run views, programs, etc. from open view results.

Dynamic Drill Down List

Maintain the file containing available 'drill to' fields for use in Dynamic Regroup/Show Detail views and Sequel Drill Down Applications.

SWI Function Authorization

Use this feature to lock or unlock access to specific Sequel Web Interface actions and features.

Get the Latest Version of Viewpoint Administrator

Viewpoint Administrator is installed with Viewpoint.

After the initial installation of Viewpoint, updates can be found on 'Your Account' page: www.helpsystems.com/user.

Check your current version by selecting **Help \About Viewpoint Administration** from the Object Display menu.

Administrator Requirements

IBM Power Systems (System i, iSeries, AS/400)

The operating system must be:

- IBM i (i5/OS, OS/400) 7.2 or higher

Viewpoint Client

Viewpoint is the Windows interface to Sequel and is used to create, access, run, and manage your Viewpoint objects (queries, reports, scripts, dashboards and so on). Viewpoint requires the following:

- A PC with at least 2GB of RAM, 250Mb of available disk space, a Pentium (or equivalent) processor, graphics resolution of 800 x 600 or higher along with the following:

- 64-bit Windows 7/8/8.1 Professional or Windows Server 2012/2012 R2/2016 with:
  - IBM i (System i, iSeries, Client) Access for Windows version V6R1 service pack SI35607 (or higher), or V7R1 service pack SI53809 (or higher) with the following installed components:
    - Client Access Express Required Programs.
    - iSeries Navigator Base Support (an option under iSeries Navigator).
    - Commands Component (an option under iSeries Navigator - for prompting commands in the script designer).
    - OLE DB Provider (an option under Data Access).
    - To verify these components are installed, go to: Start\Programs\IBM iSeries Access for Windows\Selective Setup. On the Selective Setup window, press Next. On the Selective Setup Options window, select 'Ignore, I am only going to uninstall' and press Next (you won't uninstall, but will check if the components are installed). On the Component Selection window, verify that Required Programs is selected. Expand the iSeries Navigator node to verify that the Basic Operations and Commands components are listed and selected. Expand the Data Access node and verify that OLE DB Provider is listed and selected.
    - A System i defined in iSeries Navigator.
    - This is sometimes an issue for people who don't typically use Client Access as their emulator. If you start iSeries Navigator, you should see your System i under My Connections. To check, go to: Start\Programs\IBM iSeries Access for Windows\iSeries Navigator\My Connections.
- Microsoft .NET 3.5 or higher.

> **NOTE:**
> If you use Windows 7 (64-bit) on the Viewpoint Client, install Viewpoint into the Program Files folder '`C:\Program Files (x86)\Sequel ViewPoint[Showcase 10]`'. If you install into a different directory, make sure to use the SWI command, `SEQUELWI/SWIVPDFT`, and set the **Program File Directory** (PGMFILEDIR) parameter to the same path.

or

- Windows 10 with:
    - IBM Access Client Solutions (ACS) Windows Application Package with the following installed components:
        - Required Programs.
        - OLE DB Provider (an option under Data Access).

            To verify these components are installed, go to: Windows Settings\Apps and features OR Control Panel Programs and features. Find IBM i Access Client Solutions – Application Package and click on Change or Modify. Be patient as it can take the Install Shield wizard quite a while to open. Make sure the OLE DB Provider does not have a red x indicating it is not selected.
        - A System i defined in iSeries Navigator.
- Microsoft .NET 3.5 or higher.

Administration Control Screen

The Administration Control screen is first seen when the product is started. It provides a single point of access to the different functions that make up Viewpoint Administrator.

Choose a system from the drop down list, select one of the Administrator functions, and press **OK**.
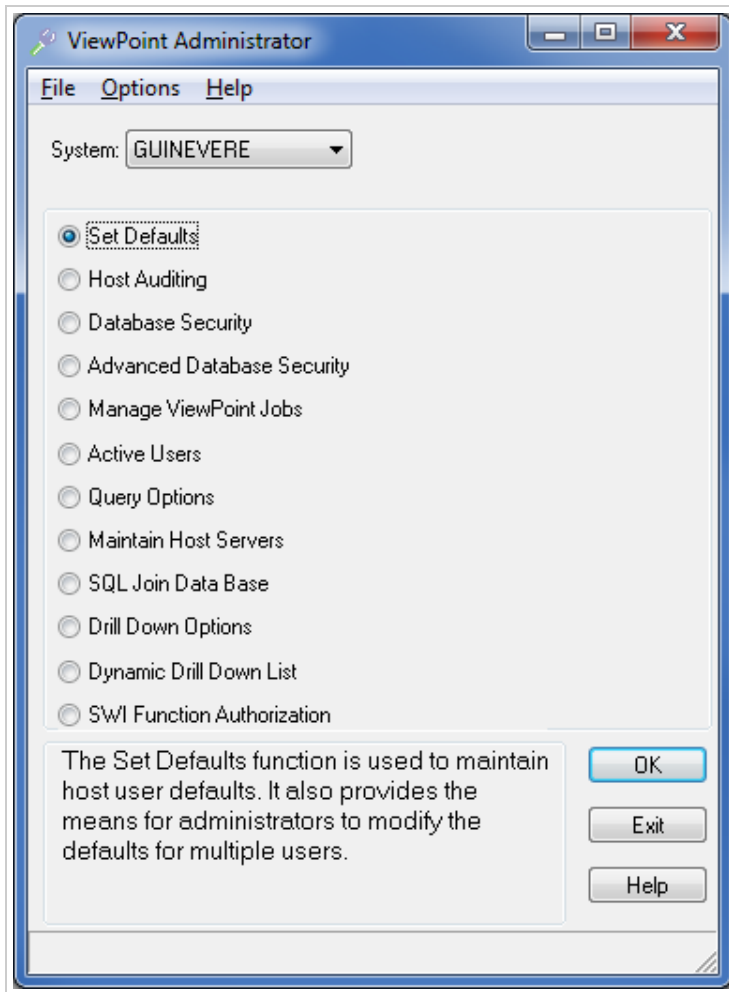
Menu Options:

File\Exit - Exit and close the Administration Control screen.

Options\Preferences... - Open the Preferences dialog to change the progress AVI and Date Range defaults.

Help\Topics - Open the on line help.

Help\About - Display Administrator version information.

Options

System - Use the drop-down list to choose which system to work with. The initial system displayed is a default setting in Viewpoint. Start Viewpoint and select **Options=>Viewpoint Options** from the menu. On the General Tab you can set the Default System.

Function Radio Buttons - Use the radio button to select which Administrator feature to access.

OK Button - After selecting a system and one of the Administrator functions, press the OK button to start.

Exit Button - Press Exit to close the Administrator.
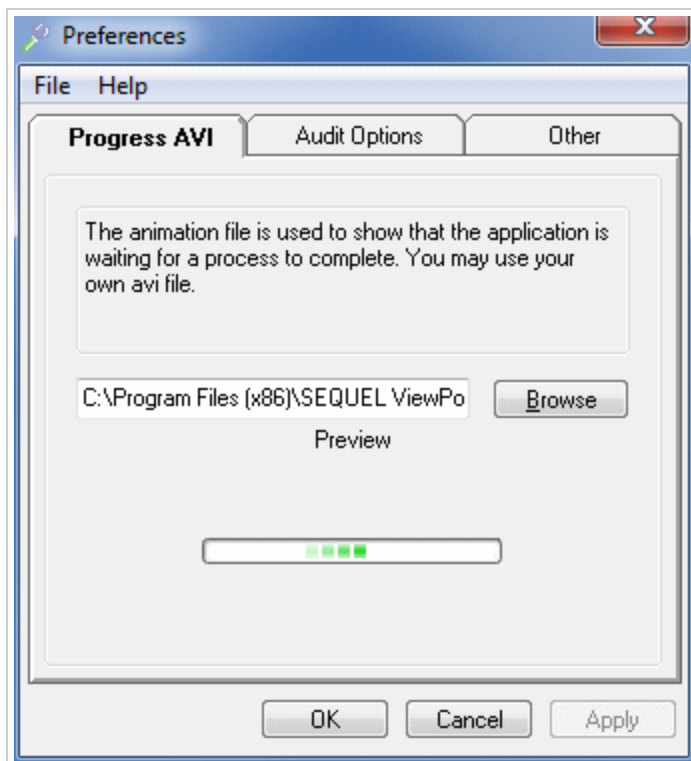
Help Button - Press Help to access the help system.

Administrator Preferences

On the Administration Control menu, select **Options=>Preferences** to access the two screens below.

Progress AVI

Use the Browse Button to select a different AVI file.

Options

Browse Button - Use the browse button to find and select a different AVI file.

Audit Options

Three different Options can be set here. These options act as 'governors' for the queries that are run for Audit Data, Audit Query, and Managing Audit Data. For each of these requests, a warning is issued if any of the values below are exceeded.
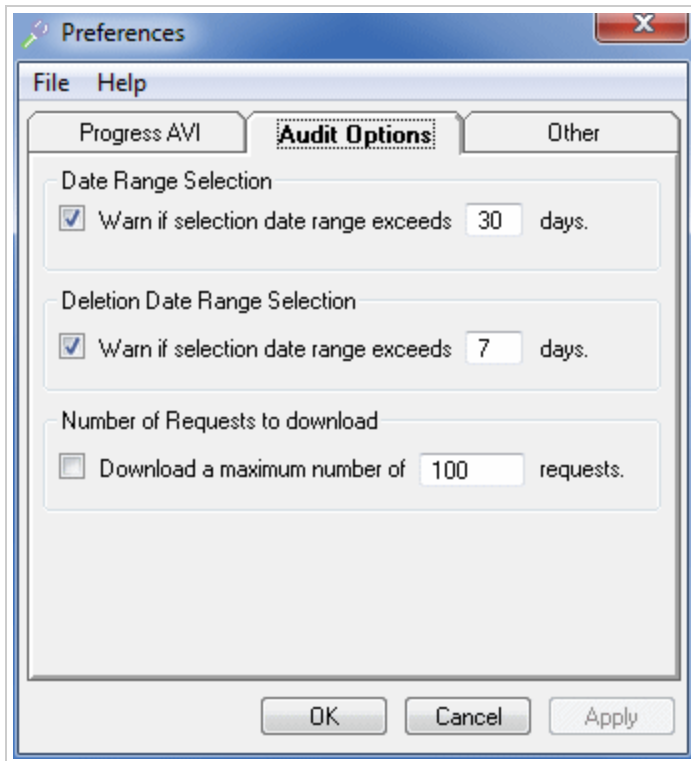
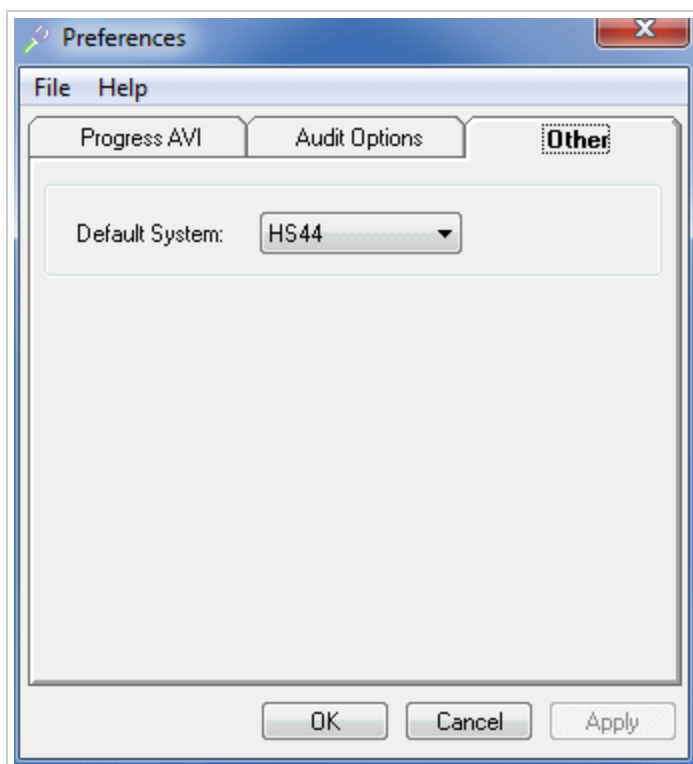## Options

Date Range Selection - Check the box to choose this option and specify the number of days.

Deletion Date Range Selection - Check the box to choose this option and specify the number of days.

Number of Requests to Download - Check the box to choose this option and specify the number of requests.

Other

Specify a default system for Administrator using the drop down list.

[Options]

Default System - Select a system as the default from the drop down list.

Administrators versus Users

Access to certain functions and entire modules of Viewpoint Administrator is controlled by the type of user accessing the module or function. There are only two classes of Sequel Users' when it comes to using Viewpoint Administrator: Administrators and Users.

Sequel Administrators:

A Sequel Administrator is a user on the system that has *CHANGE authority to the SQ#DFT data area. This allows the Sequel Administrator access to all the functions in Viewpoint Administrator.

At the system level, a user will have *CHANGE authority to the SQ#DFT data if:

- the user has *ALLOBJ authority in their user profile.
- the user is assigned a Group Profile that has *CHANGE authority to the SQ#DFT data area.
- *PUBLIC has *CHANGE authority to the SQ#DFT data area.

Sequel Users:

A Sequel User is a user on the system that has *USE authority to the SQ#DFT data area. A Sequel User can be limited further by defining them as Restricted or Unrestricted. This is set in

the Other Defaults section – 'Allow change to library defaults'.

When a user starts Viewpoint Administrator and connects to their iSeries system, Viewpoint checks to see if they are a 'Sequel Administrator'. If they are not, they will NOT have access to the following:

- They will not be able to apply any product license keys.
- In the Audit Module, they cannot add or remove audit data. They will only be able to view the audit data.
- In the Database Security module, they cannot work with the exclusion/inclusion dictionary.
- In Set Defaults they will only have access to their own defaults. They will not be presented with the Defaults Selection screen in order to maintain and create defaults for other users. If they are 'Restricted ' they cannot change the value for their default view and outfile creation libraries.

Set Defaults

Defaults Overview

Interface defaults (used by the view, table, and report designers and the main Viewpoint Object display) are created and maintained in this module of the Viewpoint Administrator.

A user specific data area containing preferred default values will be created for each Viewpoint or Sequel user. The first time a user accesses Viewpoint, the SQ#DFT "global default" data area (*DFT) will be used as the source for their default values. User data areas will be stored in the same library as the SQ#DFT data area. They will be named with the name of the user's profile.

SequelAdministrators have full access to this module. Defaults can be modified for all users, default templates can be created and applied to any user, and administrative rights can be granted to users.

SequelUsers will only be allowed to modify their own defaults.

Defaults Selection

The Defaults Selection screen is displayed after selecting 'Set Sequel Defaults' from the main Administration Control screen. Only Sequel Administrators have access to this screen. Sequel Users will be taken directly to the General Tab for their defaults.

The screen is divided into three sections to easily keep track of Templates, Administrators, and Users.

For Sequel Administrators this display provides access to the following functions:

- Create (copy), modify, delete, or apply templates.
- Modify, copy, or apply the `global' default data area (*DFT).
- Modify other user's defaults.
- Grant and Revoke administrative rights.
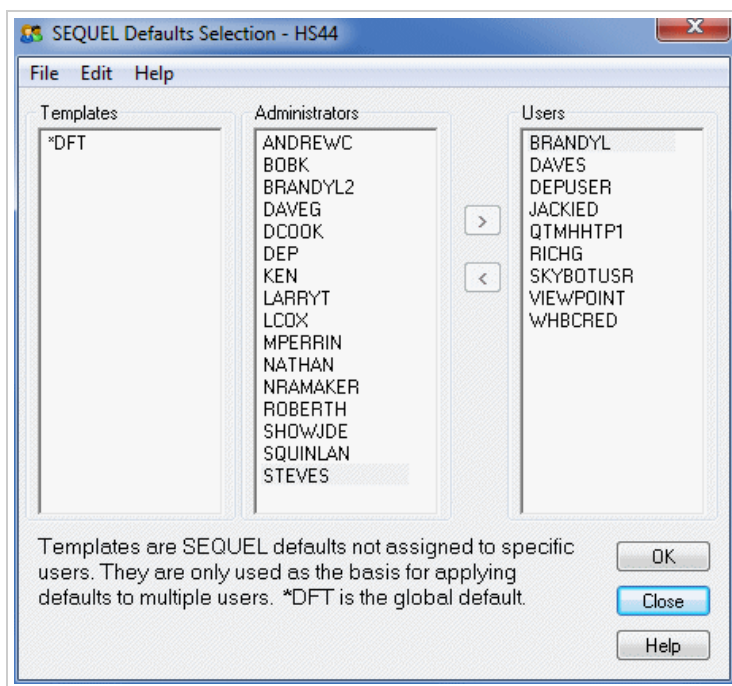
Options

Templates - Displays a list of default templates. The 'Global' default data area(*DFT) is always listed

Administrators - This section displays a list of Sequel Administrators. They have full access to the product. Administrative rights can be revoked by dragging a user from this column to the 'Users' column. Users listed here with administrative authority due to *ALLOBJ authority, a Group Profile authorization, or *PUBLIC authorization, cannot be revoked here.

Users - This section displays a list of Sequel Users. They are restricted from various parts of the product (including **this** display). Administrative rights (and full access to the product) can be granted by dragging a user from this column to the 'Administrators' column.

OK Button - Press OK to review or modify the selected template, user, or administrator.

Close Button - Press the Close button to exit the Defaults Selection screen.

Help Button - Press Help to access the on line help.

Menu Options

File \ Close - Close the Defaults Selection dialog and return to the main Administration Control screen.

File \ Refresh List - Refresh the list of users and administrators.

File \ Exit - Close the Defaults Selection dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

Working with Templates

There is always one default template in Sequel (Viewpoint) - the 'global' default data area (*DFT). With Viewpoint Administrator, you can now create your own templates. These templates can be easily created by copying the global default or any user default and saving it with a different name.

For instance, you might make a copy of the global default, change some of the settings, and name this FINANCE. Then, as new finance employees are hired you can copy the FINANCE template to their user id. Their Sequel defaults are in effect a copy of the master FINANCE template.

Templates can also be modified, deleted, and template settings can be easily applied to one or more existing users defaults.

To Create (copy) a Template:

1. Select the 'global' default data area(*DFT), an existing Template, or any existing User's Default.
2. Right click with your mouse and choose **Copy...** from the drop down menu.

    The Copy Defaults screen displays:

    ### Copy Defaults

    Create a new SEQUEL default based on ID: `SQ#DFT`

    Select User or enter new template name: `FINANCE`

    Description: `Finance Dept Defaults Template`

    To allocate SEQUEL defaults to a User Profile that does not yet have defaults assigned, select a user name from the dropdown list. For a new template, key a name and then the tab key, to enter the description.

    `OK`   `Cancel`   `Help`

3. Specify a name for the new Template and a description. Press the **OK** button when finished.
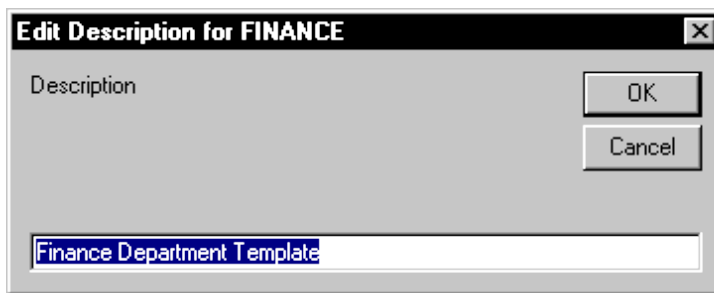
    The Templates column will have a new entry.

To Delete a Template:

1. Right click the desired Template.
2. Choose **Delete** from the drop down menu.

    You will be asked to verify your request to delete.

To Change a Template's Description:

1. Right click the desired Template and choose **Change Description** from the drop down menu.

   The Edit Description for ..... screen displays:

2. Change the existing description and press **the** OK button.

To Modify or View the Settings of a Template:

1. Select a template and press the **OK** button, or double click the template.
   The General Defaults tab for the Template displays.
2. Make any changes necessary in any of the default sections and press **OK** to exit.
   The template will now have the new changes.

To apply a Templates settings to a user:

1. Select a template and press the **OK** button, or double click the template.
   The General Defaults tab for the Template displays.
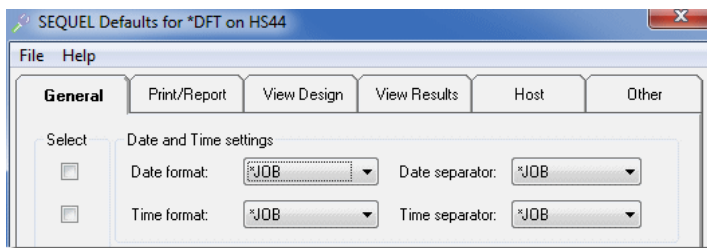
2. Check the **Select Box** to left of each setting you want to apply and press the **Apply to User(s)** button.
   A list of existing users displays:

3. Place a check next to each user you want to apply the settings to, and press the **OK** button.

Working with the Global Default Data Area (*DFT)

A global default data area is shipped with Sequel. It is always listed in the Template column of the Defaults Selection Screen as *DFT.

The first time a user on the system accesses Sequel from a 'green screen' or through Viewpoint, a copy of the global default is saved with the name of their user id.

The global default data area can be modified, copied to a user that has never tried to access Sequel, or copied as a new Template. Individual settings can be applied to one or more existing users defaults.
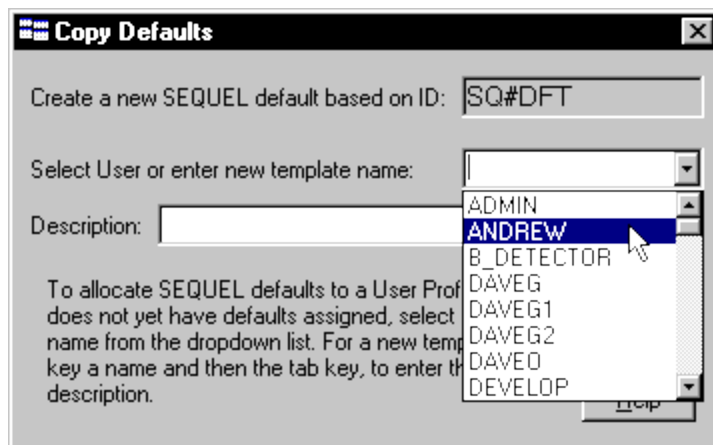
The global default cannot be deleted.

To modify the global default:

1. Double click *DFT listed in the Template column.
   The General Defaults tab for *DFT displays.
2. Make any changes necessary in any of the default sections and press **OK** to exit.
   The template will now have the new changes.

To copy the global default to a new user:

1. Select the **'global' default data area** (*DFT).
2. Right click with your mouse and choose **Copy...** from the drop down menu.
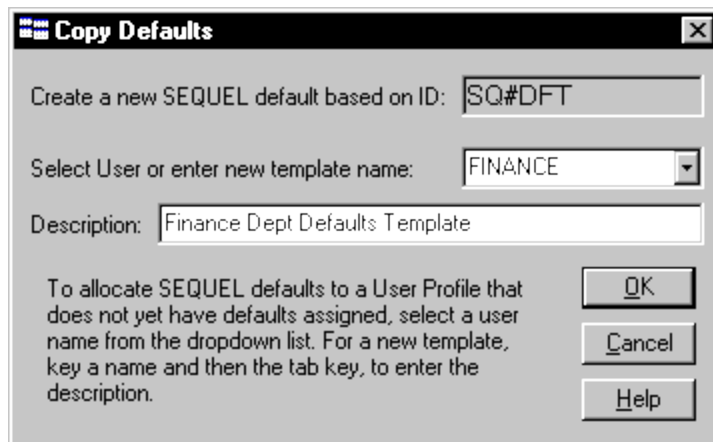   The Copy Defaults screen displays:

3. Enter a **user id** or choose one from the drop down list.
4. Enter a description and press the **OK** button when finished.

To create a Template from the global default:

1. Select the **'global' default data area** (*DFT).
2. Right click with your mouse and choose **Copy...** from the drop down menu.
    The Copy Defaults screen displays:

3. Specify a name for the new Template (a name that is not a user id) and a description.
4. Press the **OK** button when finished.
    The Templates column will have a new entry.

To apply some or all global default setting to an existing user:

1. Double click ***DFT** listed in the Template column.
    The General Defaults tab for *DFT displays:
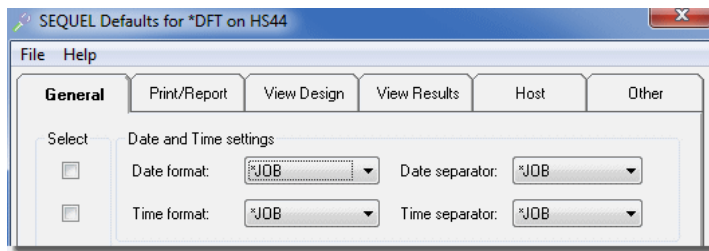
2. Check the **Select Box** to left of each setting you want to apply and press the **Apply to User(s)** button.

   A list of existing users displays:

3. Place a check next to each user you want to apply the settings to and press the **OK** button.

Working with Existing User Defaults

As a Sequel Administrator you have access to all user defaults. A user's defaults can be easily created by copying the global default, an existing template or any other existing user's default and saving it with a different name. User defaults can also be modified, deleted, and the settings from one user can be easily applied to one or more existing user's defaults. Lastly, one users defaults can be used to create a Template.

To Create (copy) a User's Defaults:

1. Select the **'global' default data area** (*DFT), an existing Template, or any existing User's Default.

2. Right click with your mouse and choose **Copy...** from the drop down menu.

   The **Copy Defaults** screen displays:
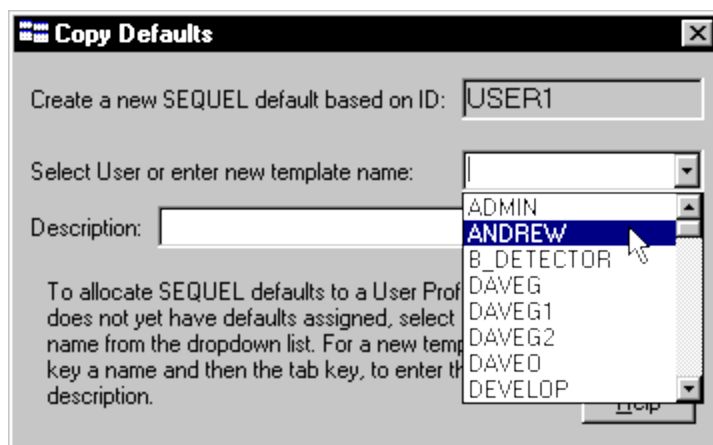
3. Enter a **user id** or choose one from the drop down list.
4. Enter a description and press the **OK** button when finished.

To Delete a User' Defaults:

1. Right click the desired user.
2. Choose **Delete** from the drop down menu.
   You will be asked to verify your request to delete.

To Change a Users Defaults 's Description:

1. Right click the desired user and choose **Change Description** from the drop down menu.
   The Edit Description for ….. displays:
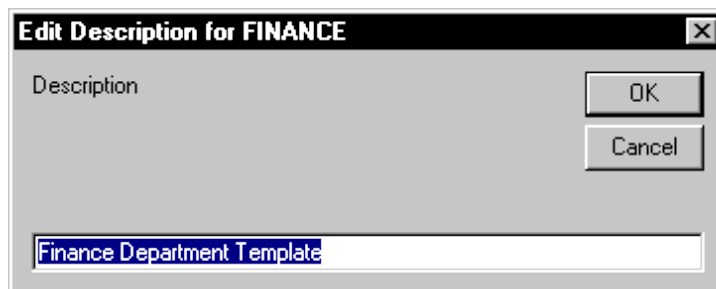
2. Change the existing description and press the **OK** button.

To Modify or View the Settings for a users defaults:

1. Select a user and press the **OK** button, or double click the user name.
   The General Defaults tab for the that user displays.
2. Make any changes necessary in any of the default sections and press **OK** to exit.
   The user's default will now have the new changes.

To apply one users defaults to another user:

1. Select a user and press the **OK** button, or double click the user name.
   The General Defaults tab for that user displays.
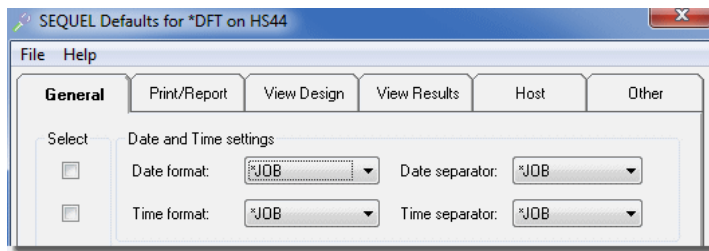
2. Check the **Select Box** to left of each setting you want to apply and press the **Apply to User(s)** button.
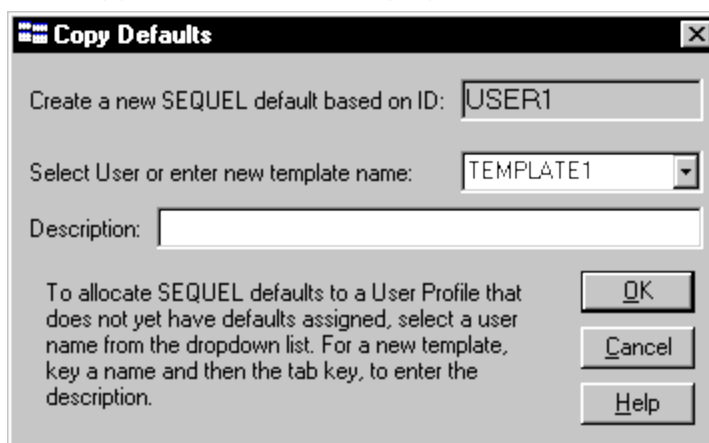
A list of existing users displays:

3. Place a check next to each user you want to apply the settings to and press the **OK** button.

To Create (copy) a Template from a users defaults:

1. Select a user and right click with your mouse. Choose **Copy...** from the drop down menu.

The Copy Defaults screen displays:

2. Specify a name for the new Template and a description and press the **OK** button. The Templates column will have a new entry.
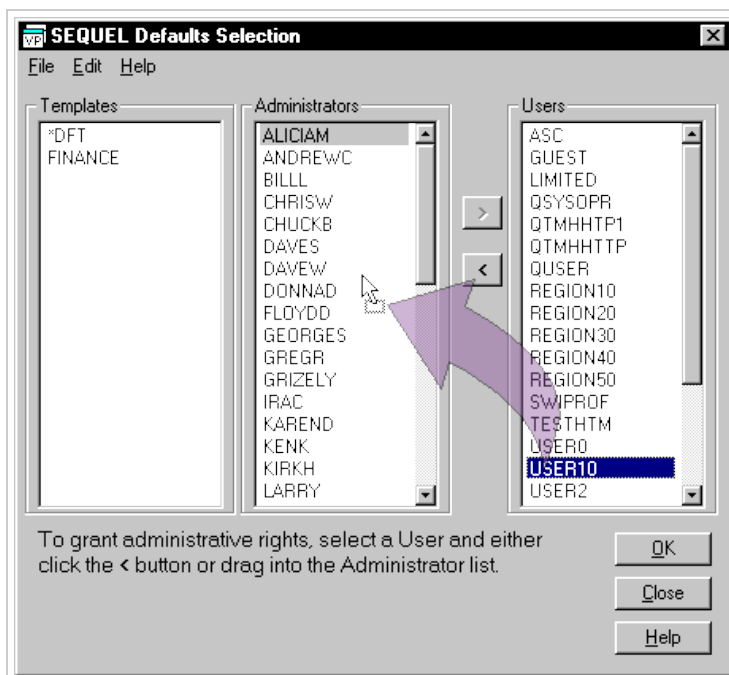
Granting and Revoking Administrative Rights

As a Sequel Administrator, you have the ability to grant administrative rights to a user or revoke administrative rights from an administrator.

> **NOTE:**
> Sequel Users do not have access to the following:
>
> - They will not be able to apply any product license keys.
> - In the Audit Module, they cannot add or remove audit data. They will only be able to view the audit data.
> - In the Sequel Field Level Security module, they cannot work with the exclusion/inclusion dictionary.
> - In Sequel Defaults they will only have access to their own defaults.

To grant administrative rights to a user, simply select the user and drag and drop them into the **Administrators** column. These 'new' administrators will now have access to the areas of the product they were previously restricted from as users.

To revoke administrative rights from an administrator, select an administrator and drag them into the **Users** Column.

> **NOTE:**
> Not all administrators can have their rights revoked. If an administrator has administrative authority due to *ALLOBJ authority, a Group Profile authorization, or *PUBLIC authorization, they cannot be revoked here. The following error is issued:
>
>
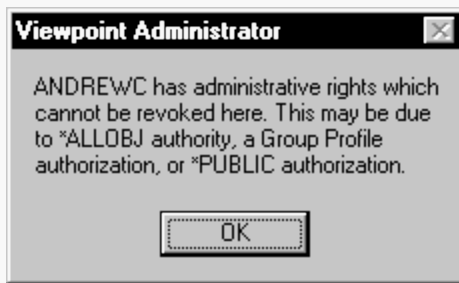
Default Parameters

For a Sequel User, the Sequel Defaults for.... screendisplays after selecting Set Defaults from the main Viewpoint Administrator screen.

A Sequel Administrator must first choose a user, template or global default from the Defaults Selection screen.
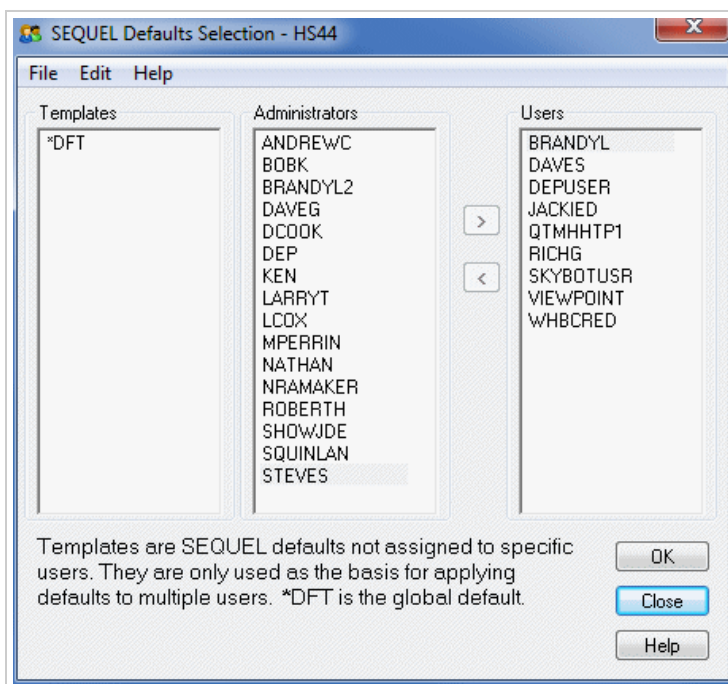
General Defaults

The defaults for a user, template, or the global default (*DFT) are divided into five sections. Click on each tab to access that section.
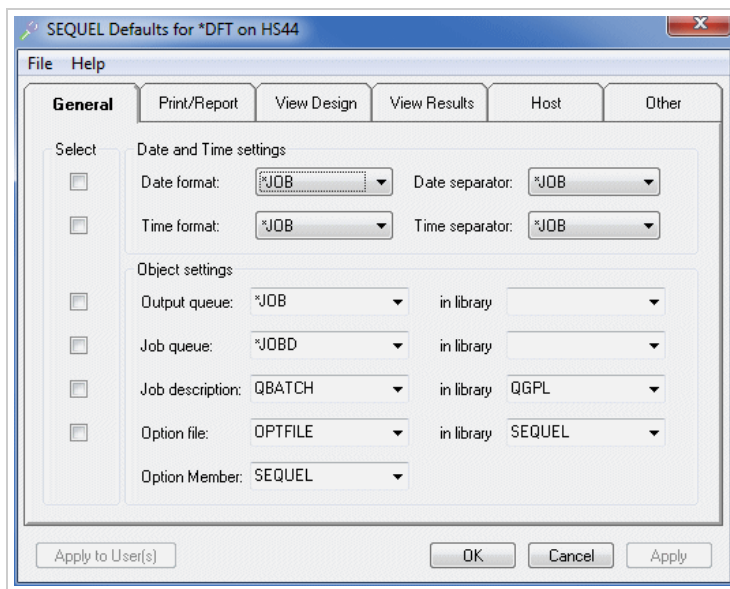
Options

Date and Time Values - Use the drop down list to specify the format and separator you want to use for date and time values in the view and report.

Output Queue - Identify the preferred output queue for printing view and report results. Indicate the queue name and library. Use the special value *JOB as the queue name and leave the library blank to indicate the job's standard output queue should be used.

Job Queue - Jobs submitted from Viewpoint will only use the job description and submit to the job queue specified on the job description.

Job Description - This job description will be used when requests are submitted for batch execution. The job description will govern the submitted job's attributes (run and output priority, etc.) in all cases where the Submit Job (SBMJOB) command's parameter default values specify *JOBD. Specify the name of a job description or use the special value *USRPRF to indicate that the job description named in the submitted job's user profile should be used.

Option File and Member - This file will be used as the source for user options by the 'Work With' commands. (in the green-screen version) In Viewpoint this option file is used for drill-down type views. Specify the file, library, and member name of the preferred option file.

Select Boxes - Sequel Administrators can select any or all settings from a template, an existing user default, or the global default data area, and apply them to other templates and users. After checking the boxes for the values you wish to apply, press the Apply to User(s) button. (described below)

Apply to User(s) - Press this button to apply any selected settings to other users or templates. This button is used in conjunction with the Select Boxes. (described above)

OK Button - Press OK to save changes and close the defaults screen.

Cancel Button - Press the Cancel button to exit without saving changes.

Apply Button - Press Apply to make any changes and leave the defaults screen open.

Menu Options:

File \ Cancel - Close the Defaults and return to the Defaults Selection screen.

File \ Select All - Checks the 'Select Box' for all parms for all tabs.

**File \ Unselect All** - Unchecks the 'Select Box' for all parms for all tabs.

File \ Exit - Close the Defaults dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

Print/Report Defaults

These defaults control attributes of printed output. Specify the standard page size and attributes by using appropriate length, width, print density, and overflow information.
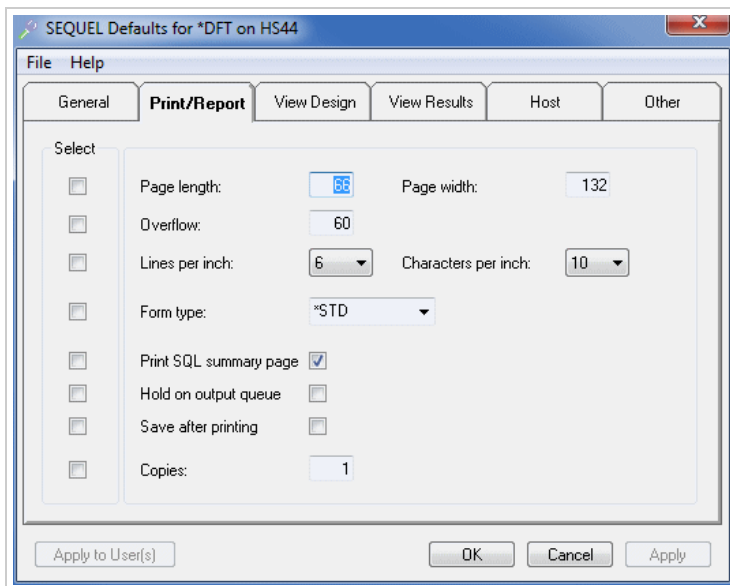
Options

Print Length - Specify a length up 255 lines. This value is determined by the paper size, orientation and lines per inch. The default values work in most cases.

Print Width - Specify a width between 1 and 378. This value is determined by the paper size, orientation, and characters per inch.

Overflow - Specify an overflow value that is less than or equal to the page length.

Lines per Inch - Specify the number of print lines per inch.

Characters per Inch - Specify the number of characters to print per inch.

Forms Type - Specify the forms type to use. *STD is the default.

Print SQL Summary Page - Check this box to print a SQL summary page with printed view results.

Hold on Output Queue - Check this box to the generated spool file in the Output Queue. The spool file will have to be released manually.

Save After Printing - Check this box to save the generated spool file in the Output Queue after it prints.

Copies - Indicate the number of copies to print.

Select Boxes - Sequel Administrators can select any or all settings from a template, an existing user default, or the global default data area, and apply them to other templates and users. After checking the boxes for the values you wish to apply, press the Apply to User(s) button. (described below)

Apply to User(s) - Press this button to apply any selected settings to other users or templates. This button is used in conjunction with the Select Boxes. (described above)

OK Button - Press OK to save changes and close the defaults screen.

Cancel Button - Press the Cancel button to exit without saving changes.

Apply Button - Press Apply to make any changes and leave the defaults screen open.

Menu Options:

File \ Cancel - Close the Defaults and return to the Defaults Selection screen.

File \ Select All - Checks the 'Select Box' for all parms for all tabs.

File \ Unselect All - Unchecks the 'Select Box' for all parms for all tabs.
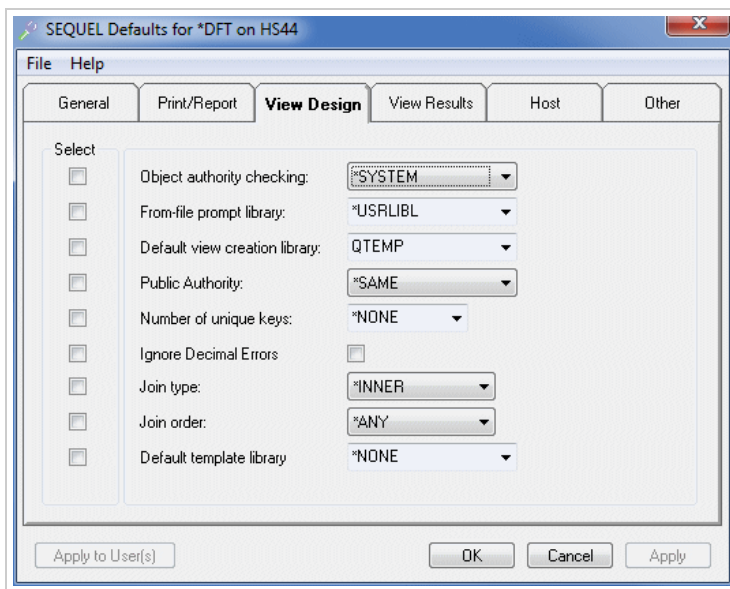
File \ Exit - Close the Defaults dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

View Design Defaults

These defaults are used when designing views in Viewpoint and with 'Classic' Sequel on the green-screen.

Options

Object Authority Checking - Choose whether standard system object authority (*SYSTEM) should be used to validate user requests, or whether Sequel's inclusion/exclusion dictionary, described in the Database Security module, should be used to augment standard object level authority. Choose one of three available levels of object authority:

SYSTEM - Use standard system object authority to validate user requests. If you use object level authority, the user will require *USE authority to the libraries, files, and views that are accessed through the user interface or "Work With" display.

SEQUEL - Use Sequel Security to supplement system object level authority. An Exclusion (or Inclusion) Dictionary is used by the design interfaces to restrict user access to libraries, files and fields. This option does not restrict complete run-time access for the user.

STRICT - Provides the same functionality as *SEQUEL plus an additional layer of security to restrict design and run-time access based on the entries in the Sequel Security Dictionary. See Enabling Sequel Security for more information.

ADS - Choose this option to use Advanced Database Security (row level) features. This option only works in conjunction with the Viewpoint Universal Driver. See the topic, *Advanced Database Security on page 79* for more information.

Limitation Note: *SEQUEL and *STRICT do not apply to users running on our Sequel Web Server (SWS). SWS user security is provided instead through Sequel Advanced Database Security (*ADS) which provides row level security in addition to the file and field security available with *SEQUEL and *STRICT.

From-file Prompt Library - Specify the default library to be used in displaying the initial list of files or libraries when the FROM prompt is selected, or when using the 'Add Files' function in Viewpoint.

Default View Creation Library - Indicate the default target library to be used when views and output files are created. A restricted user will not be able to change this value, or the From-file Prompt Library above.

Public Authority - Specify the value you want Sequel to supply as the public authority (AUT) parameter when views and reports are created. This authority will be given to the users who have no specific authority to the view and without specific authority granted to their user profile group. Use on of the following values:

*SAME: Indicates that the current attributes should apply to the new object. If the view or report does not exit, the command default for the AUT parameter is used.

*LIBCRTAUT: Public authority is taken from the value specified on the Create Authority (CRTAUT) parameter of the library into which the view or report is being created.

*USE: Allows other users to examine and run the view or report.

*ALL: Allows others to examine, run, and change the view or report.

*EXCLUDE: Prevents other users from accessing the view or report in any way.

Number of Unique Keys - If an ORDER BY clause is specified, UNIQUEKEY can be used to retrieve only the first record in a series that matches a given ordering value. The parameter is ignored unless the ORDER BY clause is specified. Refer to the description of the ORDER BY clause in the Structure of Sequel Statements section for a complete explanation of ORDER BY and UNIQUEKEY.

Use of UNIQUEKEY restricts the view to input operations. It is not updateable - the UPDATE and DELETE commands cannot use a view with UNIQUEKEY specified. In addition, the OPNSQLF command will not allow any open options except input (*INP).

*NONE: indicates that the uniqueness of the ordering paths not to be tested and used in retrieving the records. All records included in the view will be presented.

*ALL: specifies that the entire ordering specification should be used in the uniqueness test.

integer: only this number of fields (the leftmost being first) will be used in the uniqueness test. The remaining ordering fields are used in determining which record from the series with like values will be presented. The first record in each set will appear in the view.

Ignore Decimal Errors - Specifies how decimal data errors will be treated if they are encountered while the view is processed. A decimal data error occurs when a numeric (zoned or packed) field contains non-numeric information. Each digit position in the field must have a value from 0-9 and the sign portion of the field must have a range from A-F.

*NO: decimal data errors will not be ignored. Processing may or may not continue depending on the type of operation being performed.

*YES: decimal data errors will be ignored and processing will continue when possible. Each invalid decimal digit will be replaced with a zero digit, an invalid sign will be coded as a positive sign.

Join Type - Controls what happens when a multi-file (join) request is made, and no secondary records can be found to match a given primary record. The value specified for the JTYPE parameter will affect join clauses for which no specific join type is provided. That is, if the query specifies join clauses as specifically INNER JOIN, PARTIAL OUTER JOIN, or ONLY DEFAULT JOIN, the join type keyword will have no effect.

*INNER: extraneous primary records will be dropped from the view. Only records that match all joining criteria will be returned to the user.

*PARTOUT: primary records are included and missing secondary records will be filled with default values (usually blanks and zeros) when the joined record is created.

*ONLYDFT: only the primary records which do not have a matching secondary will be included in the view. For example, if you needed to know all the parts which are not currently on order you could construct a query joining the part master to the order file. Requesting *ONLYDFT will show all records in the primary (part master) which have no correspondent in the secondary (order file).

The JTYPE parameter cannot be used unless the JOIN BY clause is specified. You cannot acquire either partial outer or only-default join results if the joining specification is placed in the WHERE clause.

Join Order - Controls the order which is used in joining files together. It is ignored unless JTYPE (*INNER) is specified. Sometimes the system will be able to improve performance of the query if it is given the freedom to choose the order of the join. An inner join will produce the same record set regardless of which file is used as primary, secondary, etc. but the order of the records presented to the user may be different.

*ANY: indicates that the system has the freedom to choose the joining order.

*FILE: the first file specified in the FROM clause will be used as the primary file, and all others as secondary files. This value is always assumed when the JTYPE parameter indicates *PARTOUT or *ONLYDFT.

Default Template Library - Specify the library that contains view templates for the user. In conjunction with this setting, you should set the user's Assistance Level to *LIMITED (9). This setting is compatible with views that don't use *SEQUEL syntax (R11M11 and higher).

Select Boxes - Sequel Administrators can select any or all settings from a template, an existing user default, or the global default data area, and apply them to other templates and users. After checking the boxes for the values you wish to apply, press the Apply to User(s) button. (described below)

Apply to User(s) - Press this button to apply any selected settings to other users or templates. This button is used in conjunction with the Select Boxes. (described above)

OK Button - Press OK to save changes and close the defaults screen.

Cancel Button - Press the Cancel button to exit without saving changes.

Apply Button - Press Apply to make any changes and leave the defaults screen open.

Menu Options:

File \ Cancel - Close the Defaults and return to the Defaults Selection screen.

File \ Select All - Checks the 'Select Box' for all parms for all tabs.

File \ Unselect All - Unchecks the 'Select Box' for all parms for all tabs.

File \ Exit - Close the Defaults dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

View Results Defaults

These defaults are used when creating files from a views results.
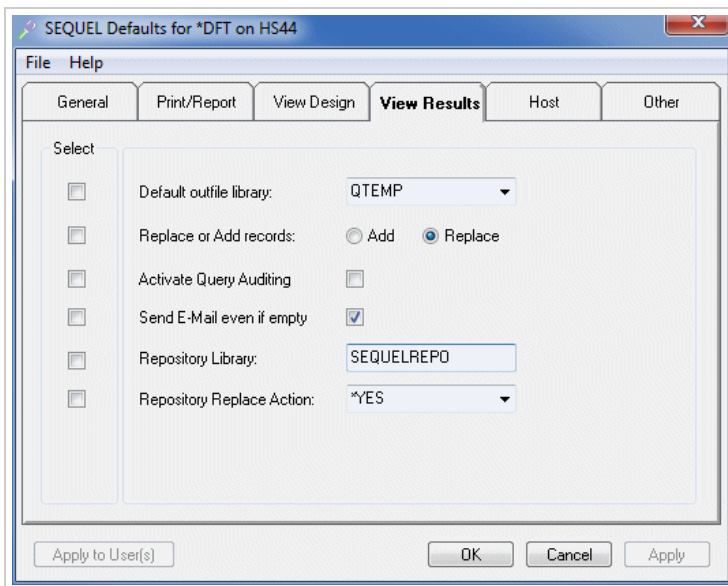
Options

Default Outfile Library - Indicate the default target library to be used when output files are created. A restricted user will not be able to change this value.

Replace or Add Records - Specify whether records produced by a view should normally replace or add to records that already exist in the output file created.

Activate Query Auditing - This value controls whether the user's requests will be audited. Check the box to cause all requests to be audited. Refer to the Audit Module section for more information on auditing.

Send E-mail Even if Empty - When sending view output via email, check this box to send the email even if the view returns zero records.

Repository Library - This library stores user space Viewpoint objects (views, reports, scripts) created by the C&DS migration process, by importing Showcase objects into Viewpoint, or by saving Viewpoint objects to the Viewpoint Repository. The value defaults to SEQUELREPO which is created during install. In most cases, objects in this library will be referenced by a corresponding Viewpoint file (a shortcut with a .vpt* extension) in the Viewpoint Repository (on the IFS).

> If the Repository Replace Action default (below) is set to *VER, copied versions of objects created during a save-and-replace operation are also stored in this library.

Repository Replace Action - Select whether to overwrite existing host objects with or without making a copied version of the object for commands that use 'implied versioning' such as DSNVIEW, DSNREPORT, DSNSCRIPT, and Viewpoint as well as commands that explicitly specify REPLACE(*DFT) such as CRTVIEW, CRTSRIPT EXECUTE[VPT], and REPORT [VPT].

> ***YES** - Replace an existing object with a new object.

> ***VER** - Replace the original object with a new version while creating a 'versioned' copy of the original. Host object versions are stored in the library specified by the Repository Library default (above), and tracked in the SEQUEL/SQVRSNUS file. Output objects are stored in the /prod_lib_name/history/XXXX (where XXXX is the library specified by the user's Repository Library default) folder on the IFS, and tracked in the SEQUEL/SQVRSNSTMF file. **Note**: You must create the SEQUELREPO subfolder under the /prod_lib_name/history folder to create output object versions.

Select Boxes - Sequel Administrators can select any or all settings from a template, an existing user default, or the global default data area, and apply them to other templates and users. After checking the boxes for the values you wish to apply, press the Apply to User(s) button. (described below)

Apply to User(s) - Press this button to apply any selected settings to other users or templates. This button is used in conjunction with the Select Boxes. (described above)

OK Button - Press OK to save changes and close the defaults screen.

Cancel Button - Press the Cancel button to exit without saving changes.

Apply Button - Press Apply to make any changes and leave the defaults screen open.

Menu Options:

File \ Cancel - Close the Defaults and return to the Defaults Selection screen.

File \ Select All - Checks the 'Select Box' for all parms for all tabs.

**File \ Unselect All** - Unchecks the 'Select Box' for all parms for all tabs.

File \ Exit - Close the Defaults dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

Host Defaults

These defaults are used in Viewpoint for connecting to remote databases and in Administrator when defining remote database entries.
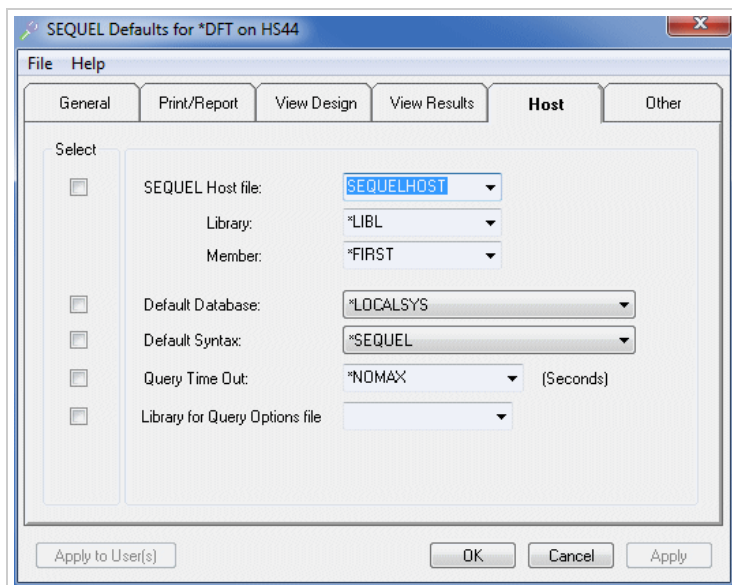
Options

Sequel Host File (library, member) -Select the file name, library and member containing remote database server entries.

Default Database - Use this Parameter to specify the default database. For queries running on the local machine, this parameter allows selection of the faster SQL Query Engine (SQE) which can offer dramatic performance improvement for longer running queries. Other queries can be created to run against any other remote system that supports DDM, CLI or JDBC access that we can connect to through the local machine.

*SEQUEL - The SQL statement must use Sequel statement syntax and the resulting view is intended to run on the local machine using the CQE processor. At runtime, the view may be run using the SQE processor by specifying SERVER(*LOCAL/*LOCALSYS) as long as automatic conversion can take place.

*LOCAL - The SQL statement contains *SEQUEL or native SQL/400 statement syntax and the request will be processed (using SQL naming – lib.file) on the local machine. The default schema (usually the library with the same name as the current user, if it exists) will be used to resolve the library name of unqualified UDFs or files in the FROM clause. If the statement is written using *SEQUEL syntax, the SYNTAX parameter must specify *SEQUEL. If native syntax is provided, the SYNTAX parameter must specify *SERVER. The resulting view will be run by the machine using the SQL Query Engine (SQE).

*LOCALSYS - The SQL statement contains *SEQUEL or native SQL/400 statement syntax and the request will be processed (using system naming or *SYS – lib/file) on the local machine. The library list of the current job will be used to resolve the library name of unqualified UDFs or files in the FROM clause. If the statement is written using *SEQUEL syntax, the SYNTAX parameter must specify *SEQUEL. If native syntax is provided, the SYNTAX parameter must specify *SERVER. The query will be run by the machine using the SQL Query Engine (SQE).

server-name - The SQL statement will be processed on a remote database server. The server-name must correspond to a valid server definition in the SequelHost file.The SQL statement can be written in *SEQUEL or in the native statement syntax for the specified database server. If written in *SEQUEL, the following SYNTAX parameter must specify *SEQUEL.

Default Syntax - This parameter specifies the specific SQL syntax used in the SQL statement. The SERVER and SYNTAX parameters work together to allow for designing views using *SEQUEL syntax using elements such as JOIN, CVTDATE and named references to derived fields while connecting to a remote database or local machine. For local queries, this also allows using *SEQUEL syntax for ease of use while running the query against the faster SQE.

*SAME - The syntax specified when the view was created will process the request. If an SQL statement is specified, then this Parameter will be treated like SYNTAX (*SERVER).

*SERVER - The SQL statement is written in the syntax of the database (Sequel, MySQL, SQLServer, Oracle, etc.) specified on the SERVER Parameter. No conversion from *SEQUEL to native SQL takes place.

*SEQUEL - The SQL statement is written and saved in *SEQUEL syntax. At runtime, if a SERVER other than *SEQUEL is specified, the statement is automatically converted to the standard SQL syntax of that database (MySQL, SQL Server, Oracle, etc.); references to multi-member files, multi-format files and ambiguous field names (unqualified field names that exist in more than one file in the FROM clause) cannot be converted and will cause the execution of the view or SQL statement to fail. See our SequelReference Guide appendix for a more complete list of *SEQUEL features that will not automatically convert to native SQL.

Query Timeout - This value applies to Viewpoint and Sequel Web Interface jobs, and s specifies a limit for database queries allowed to be started based on the estimated number of elapsed seconds that the query requires to process. If the estimated time limit is exceeded, the query will not be run and a cancel message will be sent to the job.

> **blank** - Blank indicates the QAQQINI Query timeout setting will be used.

> ***NOMAX** - There is no maximum number of estimated elapsed seconds.

> ***SYSVAL** - The query time limit is obtained from the system value QQRYTIMLMT.

Select Boxes - Sequel Administrators can select any or all settings from a template, an existing user default, or the global default data area, and apply them to other templates and users. After checking the boxes for the values you wish to apply, press the Apply to User(s) button. (described below)

Apply to User(s) - Press this button to apply any selected settings to other users or templates. This button is used in conjunction with the Select Boxes. (described above)

OK Button - Press OK to save changes and close the defaults screen.

Cancel Button - Press the Cancel button to exit without saving changes.

Apply Button - Press Apply to make any changes and leave the defaults screen open.

Menu Options:

File \ Cancel - Close the Defaults and return to the Defaults Selection screen.

File \ Select All - Checks the 'Select Box' for all parms for all tabs.

File \ Unselect All - Unchecks the 'Select Box' for all parms for all tabs.

File \ Exit - Close the Defaults dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

Other Defaults

These are some miscellaneous defaults related to authority and host settings.
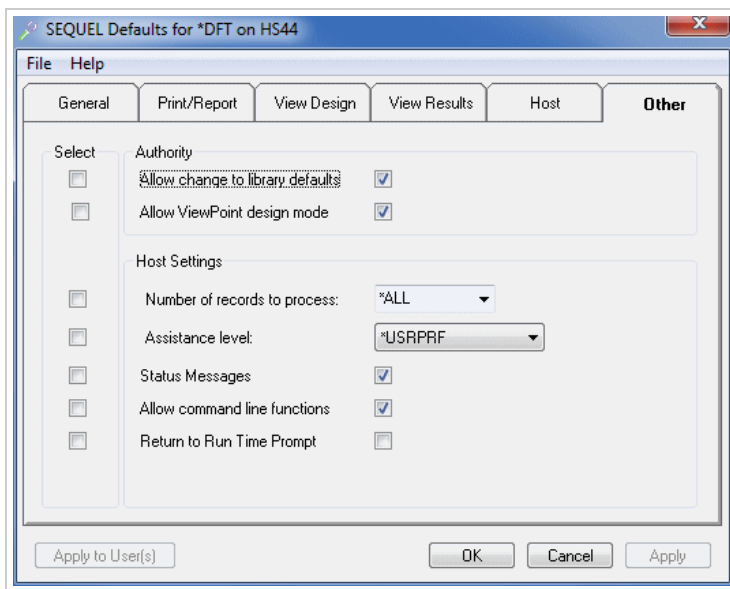
Options

Allow Change to Library Defaults - This setting controls whether a user can set their default for view, file, and FROM-prompt libraries. Once this is set by Sequel Administrator, a Sequel User is considered 'restricted'.

Allow Viewpoint Design Mode - Check this box to allow a user to design views in Viewpoint.

Number of records to process - When creating an output file, indicate the limit of the number of records that should be processed or specify *ALL to indicate that all records selected by the view should be placed into the file.

Assistance Level - Choose the assistance level (the number corresponds to the level for the host interface) for the Viewpoint view designer. Each controls the interface used, and provides varying degrees of access to different design functions.

> ***LIMITED** (9) - If the Default Template Library is set to *NONE, this assistance level forces view creation and modification to use the View Builder. Access is denied to the view designer's SQL and Files & Fields tabs. The Actions tab is presented upon view completion.
> If the Default Template Library specifies a library, this assistance level forces the user to use the New View Wizard and view templates to create new views.

> ***BASIC** (1) - View creation and modification uses the View Builder. Access is allowed to the view designer's SQL and Files & Fields tabs. The Actions tab is presented upon view completion.

> ***INTERMEDIATE** (2) - View creation and modification uses the View Builder. Access is allowed to the view designer's SQL and Files & Fields tabs. The view designer Files & Fields tab is presented upon view completion.

> ***ADVANCED** (3) - View creation and modification uses the standard view designer. Access is allowed to the view designer's SQL and Files & Fields tabs. The view designer Files & Fields tab is presented upon view completion.

This chart summarizes the assistance level options:

Assistance Level	Full Designer	View Builder	Template Wizard
*LIMITED (9) without Template Library		X[1]	
*LIMITED (9) with Template Library			X[1]
*BASIC (1)		X[1, 2]	
*INTERMEDIATE (2)		X[2, 3]	
*ADVANCED (3)	X		
1 - Display Actions tab on Finish.			
2 - Access to SQL and Files & Fields tabs.			
3 - *SEQUEL, *LOCAL, *LOCALSYS available in Data Sources tab.			

Status Messages - Check this box to show status messages in the green-screen design interface.

Allow Command Line Functions - Check this box to display a command line in the 'Work Sequel' display.

Return to Run Time Prompt - Check this box to force run-time prompted views to return to the prompt display. (repeatable run)

Library for Query Option File - Specify the library that contains the copy of the QAQQINI file to use.

Select Boxes - Sequel Administrators can select any or all settings from a template, an existing user default, or the global default data area, and apply them to other templates and users. After checking the boxes for the values you wish to apply, press the Apply to User(s) button. (described below)

Apply to User(s) - Press this button to apply any selected settings to other users or templates. This button is used in conjunction with the Select Boxes. (described above)

OK Button - Press OK to save changes and close the defaults screen.

Cancel Button - Press the Cancel button to exit without saving changes.

Apply Button - Press Apply to make any changes and leave the defaults screen open.

Menu Options:

File \ Cancel - Close the Defaults and return to the Defaults Selection screen.

File \ Select All - Checks the 'Select Box' for all parms for all tabs.

File \ Unselect All - Unchecks the 'Select Box' for all parms for all tabs.

File \ Exit - Close the Defaults dialog and exit the Administration Control screen.

Help \ Topics - Open the on line help.

Help \ About - Display Administrator version information.

Host Auditing

Auditing Overview

The Host Auditing module lets you keep track of the Viewpoint requests that are run on your system. Once the auditing module is installed and enabled, it will record information about each Viewpoint view or SQL statement that accesses records in your database. By keeping track of each request, you can find out:

- Who is using Viewpoint the most (or least)
- When are the peak use times
- How much impact Viewpoint use is having on your system
- What access paths are being created on which files[1]
- How much time is it taking to create access paths[1]
- Which files are used most (or least) by Sequel users[1]
- What data modification (UPDATE, DELETE, INSERT) is done

In short, the auditing features give you a way to monitor your investment in Sequel. The inquiries and reports help you get the most out of Sequel by showing you where it is being used heavily and how it affects your system's resources. Using the auditor's inquiry and analysis tools, you can effectively manage your query environment.

Although the auditing module contains several inquiries and reports, you may want to create your own Viewpoint views and reports (or HLL programs) to present the audit data exactly as you want to see it.

The auditing system collects these details for each request:

- Start and end date/time (timestamp) for the function
- Total CPU time required
- Number of I/O operations performed
- User profile, job and job number
- SQL statement, view, and report name used
- Execution parameters (optimization, join type, etc.)[1]
- Physical and logical files involved in the request[1]
- Access path usage (keys used, build time, file sharing)[1]
- Sequel command run by the request
- Optimization and implementation messages[1]

Accurate information is kept for each request. Execution information is retrieved from the job before and after the request executes. CPU and elapsed times do not include any time necessary to start or end the debug environment. They do include the resources necessary to process the display, printer and/or database files associated with the request.

Times and values for Open Sequel File (OPNSQLF) requests reflect only the steps necessary to open the data path. Because Sequel's programs return control when the query data path is

opened, statistics about the processing of the data cannot be included. The actual CPU time and number of I/O operations should be significantly higher than shown in the auditing record.

Once the information has been collected and placed into the audit database, you can use Sequel's inquiries and reports (or your own) to review it.

1 This information is not collected for remote database views (SQLVIEWM), including views designed to run as *LOCALSYS.

How the Auditing Process Works

There are three phases to the auditing process: collection, distribution and analysis.

Data Collection

All audit information is sent to an OS/400 journal and collected in a receiver. The journal and its receiver are automatically created when the auditing module is installed. Entries are sent into the journal by the kernel and report writing functions that use Sequel views and SQL statements to access your data. Once auditing is enabled, information about each request is sent to the journal each time a Sequel data access command (DISPLAY, EXECUTE, REPORT, INSERT, etc.) processes a view or SQL statement.

The "switch" that controls the auditing process is kept in each user's default data area. This means that you can collect auditing data for some users and not for others. The auditing module 'Set Audit Defaults' lets you review and change the settings for each user. A user's audit switch setting can also be viewed (and changed) using the Set Defaults module of Viewpoint Administrator.

Each time an audited user makes a Sequel data request, the following steps occur:

- The user's job is placed into debug mode. This causes detailed messages about query implementation and optimization to be recorded in the job log.
- The beginning timestamp is noted.
- The query request is completed.
- The ending timestamp is noted.
- Journal entries are created for each optimizer and implementation message generated during the query. A summary entry containing the starting and ending timestamp, SQL statement and view/report used, etc. is also created.
- If the job was not already in debug mode when the request began, debug mode is ended.

The auditing process adds a small amount of overhead to the queries of audited users. In most cases, the total time required to start and end the debug mode, receive messages and create the journal entries should be about 2 seconds per request.

Data Distribution

The journal receiver will collect several entries for every Sequel request performed by audited users. You must periodically run the Analyze Audit Data (ANZAUDDTA) command to recover the information in the journal receiver and distribute it to the files in the audit database. The Manage Audit Data option, runs the ANZAUDDTA command after selecting whether to add or

remove data. The command should be run regularly, perhaps daily, and can be scheduled through an automatic job scheduling system.

When the ANZAUDDTA command is run it creates a new, "empty" receiver and attaches it to the journal. It copies the entries from the old receiver into a holding file (CPIALL) and then distributes them to the various auditing files (CPIxxxx). Each audit file holds data for one particular type of message generated by the query optimizer. The QRYSUM file holds summary data that records total query time, number of records accessed, SQL statement, etc. for each audited request. When the distribution step completes successfully, the data in the holding file is cleared.

The ANZAUDDTA command runs under commitment control. All changes to the audit files are committed when the distribution step completes. If the job is ended before it completes, it can be restarted without losing or duplicating any audit information simply by resubmitting the ANZAUDDTA command.

Data Analysis

Once the information has been distributed to the audit database, the inquiry and reporting programs can be run. Several levels of summary information are available. Complete detail information can be acquired for every query that has been audited. The auditing reports and inquiries are described in the following sections:

Auditing Functions

The Sequel Auditing screen is displayed after choosing a system and selecting the Sequel Audit function from the main Viewpoint Administration screen.
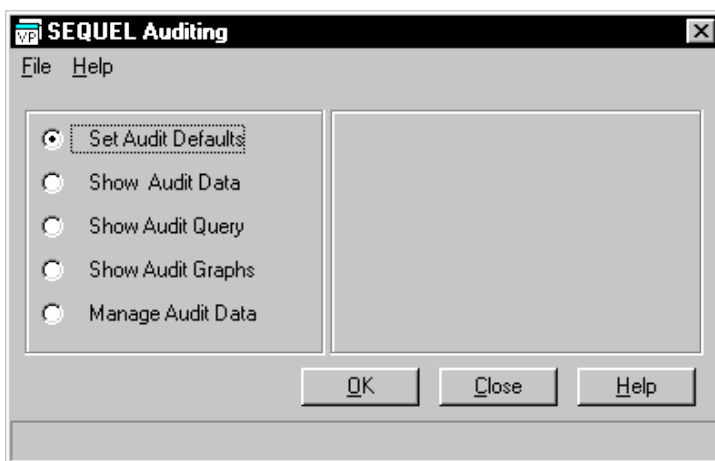
This screen provides access to the following Auditing functions:

Set Audit Defaults

This option allows Sequel Administrators to view and set the audit switch for Sequel users. Auditing can also be set through the Viewpoint Administrator Set Defaults module in the View Results section.

Show Audit Data

This option lets you view the information collected in the Audit Database. The data can be displayed by user, object, job name and access path.

Show Audit Query

This option provides an easy way to tailor a more specific request for viewing the information collected in the Audit Database. A dialog will prompt for selection criteria.

Show Audit Graphs

This function summarizes the information Audit Database in the form of charts. The data can be graphed by day, week, month and year.

Manage Audit Data

Sequel Administrators will use this function to add or delete data in the Audit Database. *USE authority to the ANZAUDDTA command is required in order to use this function.

Set Audit Defaults

The Set Audit Default option gives you an easy way to view and modify the audit switch for Sequel users. Check the box next to a user to set their default to Activate Query Auditing.

You can also access the View Results Defaults to change a user's audit value, but you will probably prefer to use the display below.

Options

User Check Box - This change takes place instantly. Leave the box empty for standard system object authority (*SYSTEM). Check the box next to a user to set their default for Object Authority Checking to *SEQUEL—the user's name will change to blue. Check the box a second time to set their default to *STRICT—the user's name will change to red. Check the box a third time to cycle back to *SYSTEM.

Summary List Button ⊞ - Press the summary button to list users without any descriptive text.

Detail List Button ▥ - Press the detail button to display the descriptive text for each user.

Apply Button - Press the Apply button to make changes to multiple users. Use Ctrl-click to select (or de-select) multiple users, or use Shift-click to select a range of users.

Close Button - Close the user list and return to the main Audit screen.

Menu Options:

File \ Close - Close the user list and return to the main Audit screen.

File \ Exit - Close the user list and completely exit Viewpoint Administrator.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Show Audit Data

This option will display the data collected in the Audit Database. You can view both summary and detail information for Sequel requests by user, object, job name and access path. Use the radio buttons to select the type of data to review.

The sample screen below shows audit data by user. Each audited user is listed with summary values for their Sequel activity. Select a user and press the OK button, or double click a user to access the detail information collected for this user.
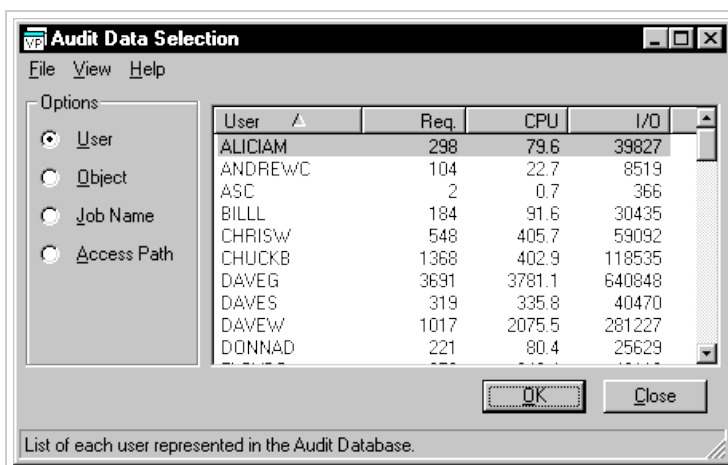
Options

Options - Indicates which type of data is currently displayed. Select a different type to change the information displayed.

Data Columns:

User - List of users that have audited requests in the database.

Req. - Number of audited requests for each user.

CPU - Total CPU seconds for each user.

I/O - Total I/O count for each user.

OK Button - Select a user in the list and press the OK button to see detailed information collected for this user.

Close Button - Close the list and return to the main Audit screen.

Menu Options:

File \ Close - Close the list and return to the main Audit screen.

File \ Exit - Close the list and completely exit Viewpoint Administrator.

View \ User..., Object..., Job..., Access Path - Change the type of data to list.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Audit Data by Object

The sample screen below shows audit data by object. These objects are files, view and reports that have been used by audited requests. Select an object and press the OK button, or double click an object to access the detail information collected for this object.
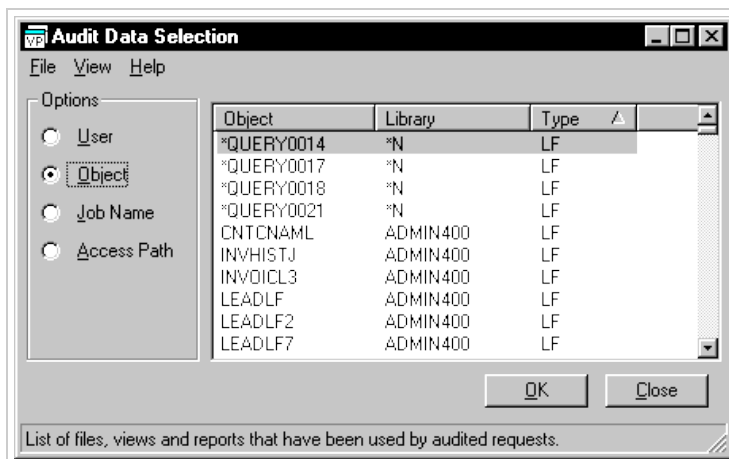
Options

Options - Indicates which type of data is currently displayed. Select a different type to change the information displayed.

Data Columns:

Object - List of files, views and reports that have been used by audited requests.

Library - Library where the object is located.

Type - Object type(LF, PF, View, Report).

OK Button - Select an object in the list and press the OK button to see detailed information collected for this object.

Close Button - Close the list and return to the main Audit screen.

Audit Data by Job Name

The sample screen below shows audit data by job name. Select a job and press the OK button, or double click an object to access the detail information collected for this job.
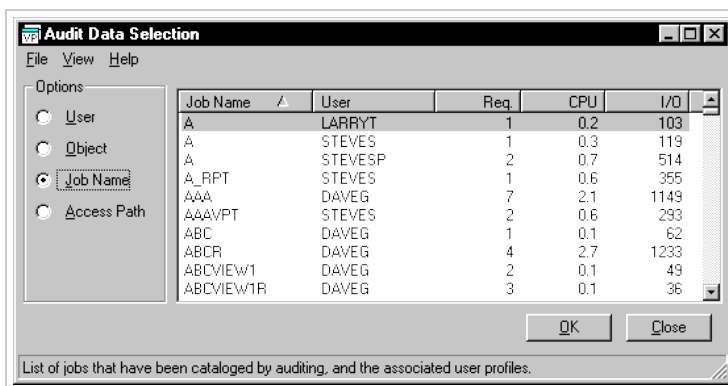
Options

Options - Indicates which type of data is currently displayed. Select a different type to change the information displayed.

Data Columns:

Job Name - List of Jobs cataloged by auditing.

User - List of the job's associated user.

Req. - Number of audited requests for each job/user.

CPU - Total CPU seconds for each job/user.

I/O - Total I/O count for each job/user.

OK Button - Select a job in the list and press the OK button to see any detailed information collected.

Close Button - Close the list and return to the main Audit screen.

Audit Data by Access Path

The sample screen below shows audit data by access path[1]. These objects are files, and their associated access paths, that have been used by audited requests. Select an item and press the OK button, or double click an object to access the detail information collected for this object.

Click on the sample screen below to review the different parameters and buttons.
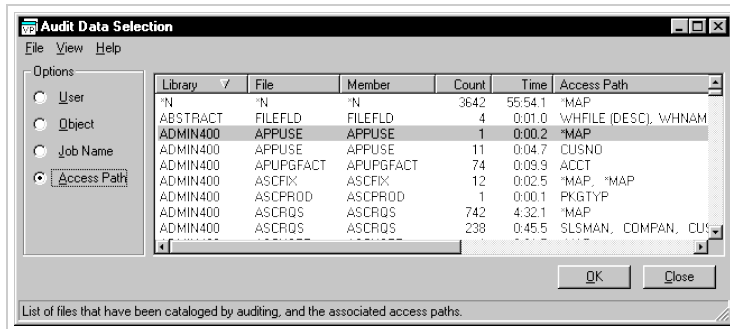
Options

Options - Indicates which type of data is currently displayed. Select a different type to change the information displayed.

Data Columns:

> Library - Library where the file is located.
>
> File - Name of files used in audited requests.
>
> Member - Member associated with the file.
>
> Count - Number of times the access path was used in an audited request.
>
> Time - Total time to create access path.
>
> Access Path - List of the fields used to create the access pass. *MAP indicates that a derived field was used for the access path.

OK Button - Select a file in the list and press the OK button to see any detailed information collected.

Close Button - Close the list and return to the main Audit screen.

Show Audit Query

Choosing Show Audit Query from the main Auditing screen will display the Audit Query Selection window below. This option lets you work with your choice of audit information. It lets you tailor a query to provide the data that will display in the Work with Audit Data display.

The screen below passes your selection criteria to a prompted Sequel view (AUDITQRY). The variables are combined with common selection requests in the view's WHERE clause. By entering values for some of the variables and omitting others you will usually be able to choose

the audit requests you want to see. After entering selection criteria, press the Run Query button to work with the summarized and detailed data.

Specify as many values as necessary to choose the data you want to see. The list of criteria will be "AND'ed" together to select the audit data.

Options

Start Date and Start Time - Specify the starting date and or time for the search. Use the drop down calendar to quickly choose a date. A warning will be issued if the number of days selected exceeds the value set in Administrator Preferences, Audit Options section.

End Date and End Time - Specify the ending date and or time for the search. Use the drop down calendar to quickly choose a date.

User Id, Job Name, Job Number - Specify values for the requests to be included. Only requests that were run by the user and/or job you specify will be allowed to appear in the inquiry. Some of these may be omitted by other values specified on the prompt.

Requests are tested for equality against the values you enter. If you choose to enter a user profile name, job name, and/or job number, you must enter them exactly as they will be found in the audit records.

View Name, Report Name -Specify the name of the view and/or report to be included. Only requests that were run using the objects you specify will be allowed to appear in the inquiry. Some of these may be omitted by other values specified on the prompt.

View Library, Report Library - The object name and library name fields are independent. You do not need to specify both. You can choose to specify a library name and omit the corresponding object name if you want to select all views (or reports) that were run from a particular library.

Aux I/O Count - Specify a range of values to be included. Only requests having a total I/O count in the range you specify will be allowed to appear in the inquiry. Some of these may be omitted by other values specified on the prompt.

CPU Time(Seconds) - Specify a range of values to be included. Only requests having a total CPU time (seconds) in the range you specify will be allowed to appear in the inquiry. Some of these may be omitted by other values specified on the prompt.

Order By - Choose one of the following fields from the drop down list to sort the data:

> **HESTSP** Starting timestamp
>
> **HECPU** Total CPU time
>
> **HEIO** Number of auxiliary I/O operations
>
> **HECMD** Sequel command used
>
> **HEJOB** Job name
>
> **HEUSER** User profile
>
> **HENBR** Job number
>
> **HERPLB** Report library
>
> **HERPNM** Report name
>
> **HEVWLB** View library
>
> **HEVWNM** View name

Sequence - Choose to sort the output ascending or descending.

Run Query Button - Press the Run Query button to retrieve audit data based on the above selection criteria.

Cancel Button - Press the Cancel button to exit the Audit Query Selection screen.

Menu Options:

File \ Close - Close the user list and return to the main Audit screen.

File \ Exit - Close the user list and completely exit Viewpoint Administrator.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Show Audit Graphs

This option presents audit data in graph form. You can control the graph type, duration and date values. You can easily move forward and backward through the data based on the duration. The graph can be printed or saved as a picture.
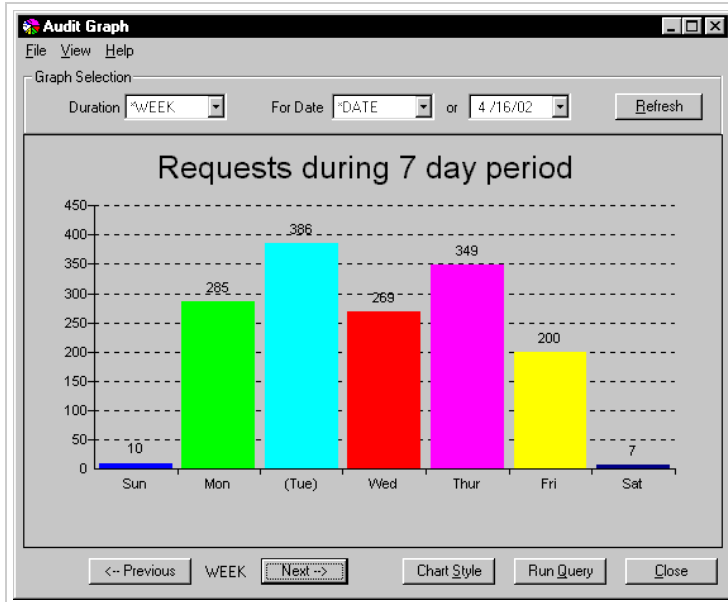
Options

Duration - Specifies the period for the graph. You can choose to see audit totals by hour within a day, by day within a week, by week within a month, or by month within a year.

For Date / Or - Specify the date to be included on the display. If you choose an hourly summary, all information will pertain to the date you specify. If you choose weekly, monthly, or yearly summaries, the date you indicate will be included in the period chosen by the duration parameter. Use the following values:

* **LAST:** The last date in the database will be used. This will be the most recent data collected, unless the DLTAUDDTA (Delete Audit Data) command has been used to remove audit information.

* **FIRST:** The first (oldest) date in the database will be used.

* **CURRENT:** Today's date will be used to determine the hourly, weekly, or monthly summaries.

* **DATE**: Enter any valid date. The date must be in your job's current date format. Use the drop down calendar to easily select a date.

Audit Details - Depending on the duration displayed you can 'drill-down' into the supporting audit data. For example, if your chart is based on a day, you can see detail for an hour.

Refresh Button - Press the Refresh button to regenerate the graph after selecting new values.

Previous Button - Move backward in the audit data one duration value. (day, month, week, year)

Next Button - Move forward in the audit data one duration value. (day, month, week, year)

Chart Style - Select a different chart style.

Run Query - While the Audit Details option above will show the audit detail for a single hour, (based on the *DAY duration) the Run Query button will show the audit detail for ALL the hours in the day.

Close - Close the graph window and return to the main audit screen.

Chart Values Right Click Menu Options:

You can right click on any of the graph values (bar, pie slice, etc,) and choose a different duration.

*DAY / *WEEK / *MONTH / *YEAR

Select a different duration value.

Menu Options:

File \ Close - Close the selection screen and return to the main Audit screen.

File \ Save Image - Save the graph as an image file.

File \ Print Setup - Display a standard Windows Print setup display.

File \ Print - Print the graph.

File \ Print(Monochrome) - Print the graph as monochrome.

File \ Exit - Close the selection screen and completely exit Viewpoint Administrator.

View \ Chart Style - Select a different chart style.

View \ Day, Week, Month, Year - Specifies the period for the graph. You can choose to see audit totals by hour within a day, by day within a week, by week within a month, or by month within a year.

View \ Previous - Move backward in the audit data one duration value. (day, month, week, year)

View \ Next - Move forward in the audit data one duration value. (day, month, week, year)

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Manage Audit Data

The Manage Audit Data option (shown below) is available to Sequel Administrators only. Use this feature to add records to or remove records from the audit database. One of two commands is invoked on the AS/400 – ANZAUDDTA (adds records) and DLTAUDDTA (removes records).

The **Analyze Audit Data** option issues the ANZAUDDTA command which retrieves the entries from the audit journal receiver and distributes them among the audit database files.

When the command completes, a new, "empty" receiver will be attached to the journal and collect the audit data. The audit database will contain all the data from the old receiver. The previous receiver is deleted during processing.

The **Delete Audit Data** option issues the DLTAUDDTA command to remove data from the audit database. Press the Advanced Delete button to define more specific deletion criteria.

Options

Analyze Audit Data - Choose this option to add records to the audit database.

Delete Audit Data - Choose this option to remove records from the audit database.

From Date - Select a starting date for deleting records.

To Date - Select an ending date for deleting records.

Advanced Delete Button - Open the Advanced Delete Option display to choose more specific delete options.

Job Queue / In Library - Specify a job queue for the submitted job.

Job Description / In Library - Specify a job description for the submitted job.

Submit Button - Press the Submit button to kick off the job to add or delete records.

Close Button - Press the Close button to exit and return to the main Audit display.
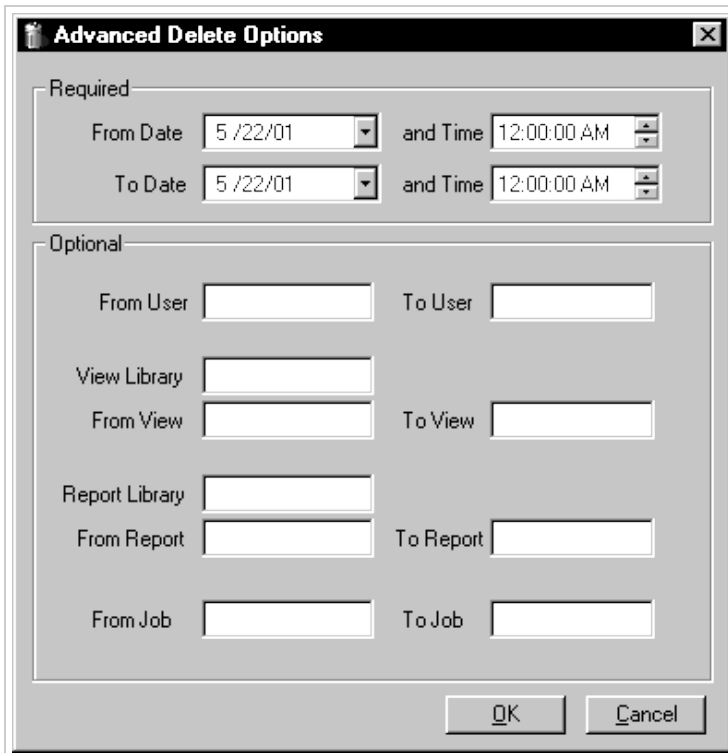
To complete successfully, the user performing the ANZAUDDTA command must have management authority (*CHANGE) to the audit journal SQAUDIT, existence rights (*ALL) to all receivers currently attached to the journal, and object insertion (*CHANGE) rights to the SEQUEL library.

The ANZAUDDTA command automatically runs under commitment control. Whether submitted to a batch subsystem or run interactively, commitment control is started when the process begins. All changes to the audit files are committed when the distribution step completes. If ANZAUDDTA is canceled or ends abnormally before completing successfully, it can be restarted without losing or duplicating any audit information. You can restart the command simply by re-executing it.

Advanced Delete Options

Use the Advanced Delete Options screen to enter more specific criteria for deleting records from the audit database.

You can define six ranges. Only the date range is required. Other ranges modify the date criteria so that only the records that meet all specified criteria will be deleted. Both the low and high values must be entered for each pair that you want to use.

Options

From Date - Specifies the lowest date to be used in selecting records to be deleted. Records with dates equal to or higher than this value will be deleted.

To Date - Specifies the highest date to be used in selecting records to be deleted. Records with dates equal to or lower than this value will be deleted.

From Time - Specifies the lowest time to be used in selecting records to be deleted. Records for requests with a beginning time equal to or higher than this value will be deleted. If you enter a value for this parameter, you must also enter a value for the TO TIME parameter.

To Time - Specifies the highest time to be used in selecting records to be deleted. Records for requests with a beginning time equal to or lower than this value will be deleted. If you enter a value for this parameter, you must also enter a value for the FROM TIME parameter.

From User - Specifies the lowest user profile value to be used in selecting records to be deleted. Records for requests that were run by a user name equal to or alphabetically after this value will be deleted. If you enter a value for this parameter, you must also enter a value for the TO USER parameter.

To User - Specifies the highest user profile value to be used in selecting records to be deleted. Records for requests that were run by a user name equal to or alphabetically before this value will be deleted. If you enter a value for this parameter, you must also enter a value for the FROM USER parameter.

View Library - Specify the library that contains the views referred to in the FROM VIEW and TO VIEW parameters.

From View - Specifies the lowest view name value to be used in selecting records to be deleted. Records for requests that were run using a view name equal to or alphabetically after this value will be deleted. If you enter a value for this parameter, you must also enter a value for the TO VIEW parameter.

To View - Specifies the highest view name value to be used in selecting records to be deleted. Records for requests that were run using a view name equal to or alphabetically before this value will be deleted. If you enter a value for this parameter, you must also enter a value for the FROM VIEW parameter.

Report Library - Specify the library that contains the reports referred to in the FROM REPORT and TO REPORT parameters.

From Report - Specifies the lowest report name value to be used in selecting records to be deleted. Records for requests that were run using a report name equal to or alphabetically after this value will be deleted. If you enter a value for this parameter, you must also enter a value for the TO REPORT parameter.

To Report - Specifies the highest report name value to be used in selecting records to be deleted. Records for requests that were run using a report name equal to or alphabetically before this value will be deleted. If you enter a value for this parameter, you must also enter a value for the FROM REPORT parameter.

From Job - Specifies the lowest job name value to be used in selecting records to be deleted. Records for requests that were run by a job name equal to or alphabetically after this value will be deleted. If you enter a value for this parameter, you must also enter a value for the TO JOB parameter.

To Job - Specifies the highest job name value to be used in selecting records to be deleted. Records for requests that were run by a job name equal to or alphabetically before this value will be deleted. If you enter a value for this parameter, you must also enter a value for the FROM JOB parameter.

OK Button - Press the OK button to process the delete request.

Cancel Button - Press the Cancel button to exit the Advanced Delete screen.

Work with Audit Data

The Work with Audit Data screen (below) is displayed as a result of 'drilling into' a user, object, or job from the Show Audit Data option , or using Run Query while in Show Audit Query and Show Audit Graph options.

The Audit Details List tab displays the audit detail requests from one of the above operations. You can also see the detail summarized and graphed by command on the Audit Command Summary tab.

Each of the line items in the list can be further drilled into to see the lowest level of information for the request (job parameters, SQL statement, messages). Double click one of the lines, or select the line and press the OK button to see the Audit Request Line Detail screen.

Options

Audit Command Summary Tab - Switch the display to see the detail summarized.

Data Columns:

Date and Time - Date and Time the request was executed.

CPU Time - Amount of CPU seconds for the request.

View / Library - Name of the Viewpoint view and library used in the request. A value of SQLEXEC is typically associated with an adhoc display.

Report / Library - Name of the Viewpoint report and library used in the request (if any).

I/O Count - Total I/O count for the request.

Command - Lists the command used in the request.

OK Button - Select a line item and press the OK button to see the <u>Audit Request Line Detail</u> screen.

Close Button - Press the close button to exit the display.

Audit Command Summary

The information from the Audit Details tab is summarized and graphed by command. The graph can be swapped between CPU time and Command usage.
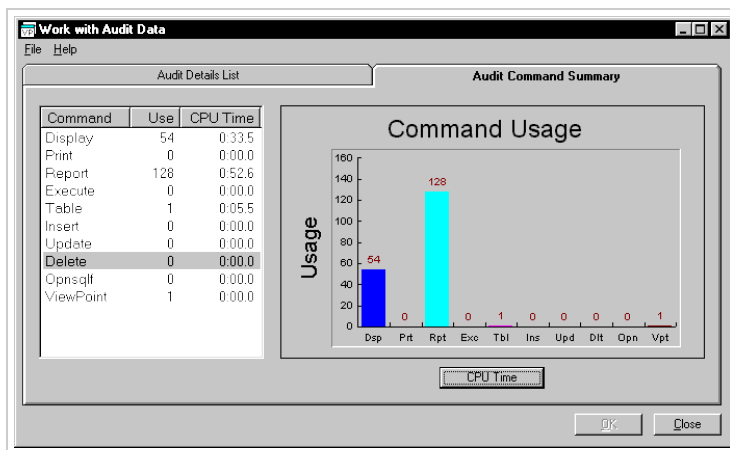
Options

Audit Details List Tab - Switch the display to see the <u>detail</u> display.

Data Columns:

> **Command** - List of the different Sequel / Viewpoint commands.
>
> **Use** - Total count for each command used.
>
> **CPU Time** - Total CPU seconds for each command.
>
> **CMD Usage / CPU Time** - Toggle the graph between CPU time per command and Usage count per command.

CMD Usage / CPU Time - Toggle the graph between CPU time per command and Usage count per command.

Close Button - Press the close button to exit the display.

Access Path Detail

The Access Path Detail screen (below) is displayed[1] as a result of 'drilling into' an access path from the <u>Show Audit Data</u> option for access paths.

Each of the line items in the list can be further drilled into to see the lowest level of information for the request (job parameters, SQL statement, messages). Double click one of the lines, or select the line and press the OK button to see the <u>Audit Request Line Detail</u> screen.

Options

Indexes - Number of indexes using the aces path.

Access Path - Access path used for the request.

Data Columns:

>**Date and Time** - Date and Time the request was executed.

>**Min:Secs** - Amount of CPU seconds for the request.

>**%Total** - Percent of the total elapsed time for the request.

>**User ID** - Name of the user for the request.

>**View / Library** - Name of the Viewpoint view and library used in the request. A value of SQLEXEC is typically associated with an adhoc display.

OK Button - Select a line item and press the OK button to see the Audit Request Line Detail screen.

Close Button - Press the close button to exit the display.

Audit Request Line Detail

Audit Request Line Detail is the lowest level information collected for a given request. This screen is accessed by drilling into one of the requests listed in the Work with Audit Data screen, or an access path listed in the Access Path Detail screen.

The Details tab lists audit, object, view description1, and date and time information. The SQL tab will show the SQL that was used in the audited request. You can copy the sql and paste it into another view or command. The Messages tab displays any query messages generated from the request.

[1] View Description information is not collected for remote database views (SQLVIEWM), including views designed to run as *LOCALSYS.

Audit Request Line Details:SQL

The SQL tab shows the SQL used in the audited request. You can copy the SQL and paste into another view or command.
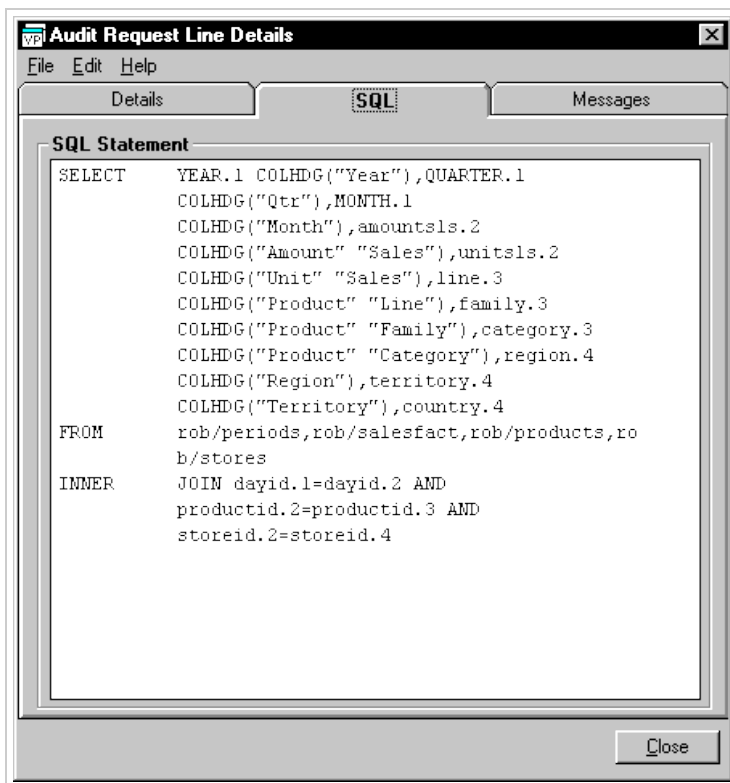
Audit Request Line Details:Messages

The Messages tab displays any query messages generated from the request[1].
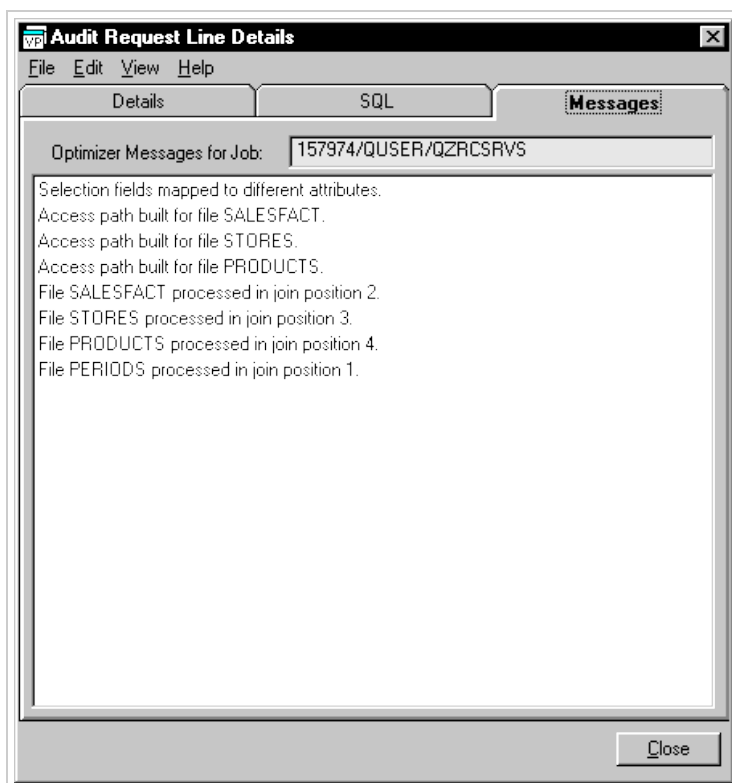
[1] This information is not collected for remote database views (SQLVIEWM), including views designed to run as *LOCALSYS.

The Audit Database

This section should help you to understand the organization of the audit database. It describes the content of each file so that you can create your own views (queries) and reports over the collected audit information. It also describes a few views that are shipped with the audit module to help you get started.

The audit database consists of several physical files and their attendant logicals. Most of the physical files contain records containing the message data for one of the many different kinds of messages generated by the query optimizer. The file name for these files begins with CPI and is derived from the message identifier of the message. The files in the audit database are listed in the table below:

Object Description

CPIALL DSPJRN output file for journal entries

CPI432A Query optimizer timed out for file &1

CPI432B Subselects processed as join query

CPI432C All access paths were considered for file

CPI432E Selection fields mapped to different attributes.

CPI432F Access path suggestion for file &1

CPI4321 Access built for file &4

CPI4322 Access path built from keyed file &1

CPI4323 Query access plan has been rebuilt

CPI4324 Temporary file built for file &1

CPI4325 Temporary result file built for query

CPI4326 File &1 processed in join position &11

CPI4327 File &1 processed in join position 1

CPI4328 Access path of file &4 was used by query

CPI4329 Arrival sequence was used for file &1

QRYSUM Query summary- elapse time, exec parms,sql

QRYTOTAL Query summary- totals

Records are inserted into the files during the ANZAUDDTA (Manage Audit Data) process. They are removed by the DLTAUDDTA command or the WRKAUDDTA program. The ANZAUDDTA process places all journal entries into the CPIALL file and then distributes them to the various CPIxxxx files. The CPIALL file will be cleared when ANZAUDDTA completes.

All the records for a given request are related through their timestamp — each request receives a unique timestamp. The master record for a request exists in the QRYSUM file. It contains execution statistics, parameter values, and the SQL statement used during the request. Records in the CPIxxxx files that are related to a given request can be found by using the timestamp listed in the master QRYSUM record.

The QRYTOTAL file is a summary file that records the number of requests and the I/O totals and CPU totals by month. The file is used to provide the bar graphs in the GPHAUDSUM command. All the records for a given request are related through their timestamp — each request receives a unique timestamp. The master record for a request exists in the QRYSUM file. It contains execution statistics, parameter values, and the SQL statement used during the request.

> **NOTE:**
> Although we encourage you to create your own views and reports on the audit data, you must not update any of these files using your own programs or views. You can easily compromise the integrity of the data by accidentally omitting one or more files from your operation, or by specifying incorrect values. The audit information is only useful if it is correct and must be maintained only through Sequel functions.

Database Security

About Database Security

Sequel includes a mechanism that lets you supplement system object authority and restrict access to database files and fields. Sequel Security is based on dictionary entries that can either be defined as Exclusion or Inclusion (not both). It is a simple two step process: define the exclusion database that limits users from libraries, files and fields, and set users' defaults to force them to use the exclusion dictionary.

You will probably want to use this feature of Sequel if your environment provides *PUBLIC authority to most files and libraries. If you want to restrict users from some of these files and allow them to access others, this will help you.

You may also want to restrict certain fields within some files from user access. Under OS/400 version 4 release 2.0, you can use Client Access to do this at the system level. Prior to V4R2, you can only use "program-defined" mechanisms like the Sequel exclusion dictionary to do this. With the Sequel security system you can identify specific fields that are to be restricted. Users can be allowed to access some fields within the file, while being denied access to others that you have identified as restricted.

Note: If you also need to apply row-level security see Advanced Database Security.

Exclusion Dictionary

Sequel security uses an exclusion dictionary that you define with a series of entries to indicate which users should be restricted from specific libraries, files and fields in your database. The exclusion dictionary is an additional filter that is applied after system object security has limited the user to objects they are normally authorized to. It does not replace system object authority but supplements it.

The exclusion dictionary consists of a series of files in the SEQUEL library. Sequel commands let you set up, maintain, and document the exclusion dictionary. Viewpoint Administrator provides easy access to the programs that are used to enter and maintain the information in the dictionary. Reporting programs can be used to document the contents of the dictionary.

Each entry in the exclusion dictionary has two parts:

USER: identifies the group of users that is covered by the entry

OBJECT: identifies the libraries, files, or fields in the database that will be excluded from use

You can specify exclusion for individual user profiles, members in a group profile, or all users on the system. Each authority search made by the user interface determines if either the specific user or the group profile or all users on the system are excluded from accessing the database object. Exclusion entries for a group profile will prohibit access for its member profiles as well.

Each dictionary entry references a library, file, or field. You can exclude access to specific libraries and prevent use of all files within them. You can also prevent use of individual files within a library and allow other files in the library to be used. Field level security can be applied to specific fields within a file; some fields can be restricted while others are not.

Inclusion Dictionary

Depending on your environment, you may prefer to use an "inclusion" dictionary that lists only the fields and files that the user is allowed to use, instead of a dictionary that lists those that the user is excluded from using. You can change the way Sequel's dictionary works by selecting **Inclusion** from the **Rules** menu. (see below)

Be careful with this option if you already have exclusions defined for users. Changing the current rule will completely 'flip' how the definitions work. For example, Bob is only excluded from the salary field in the Payroll file. If the rule is changed to Inclusion, Bob will now be allowed to use the salary field, but he will be excluded from all the other fields in the Payroll file.
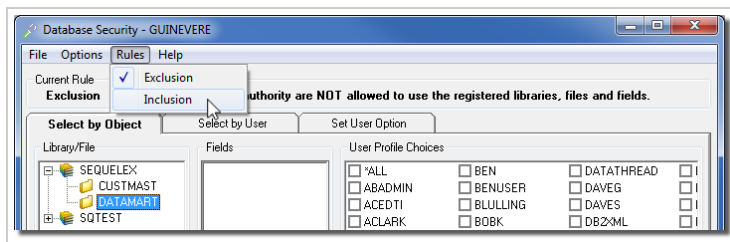
Sequel is shipped so that the dictionary and security program uses "exclusion" rules. Users are excluded from the fields listed in the dictionary.

Enabling Sequel Security

Sequel is shipped so that only standard object authority checking is performed by the system. This means that when prompting, users will be able to see the names of the libraries and files that they have operational authority to. They will be able to retrieve information from any files they have read authority to.

The Sequel security checking mechanism is enabled when *SEQUEL or *STRICT is set as a user's object authority checking value. Depending on which is applied to the user, it defines where in the product the values set in the exclusion/inclusion dictionary are enforced. The value is changed for individual users with the displays presented by the Set Sequel Default (SETDFT) command, or using the Administrator Set Defaults feature. Refer to View Design Defaults – Object Authority checking.

For *SEQUEL with unprompted views (object type SQLVIEW), restrictions are enforced only through the Viewpoint and green-screen view design interfaces. In other words, the user interface will refer to the Authority Dictionary before allowing someone to access various database elements. If no entries in the Authority Dictionary prevent them from accessing the library, file or field in question, the user will be allowed to see the item in a list and to refer to it within the query. Restrictions are not applied to statements entered through command entry, Scripts, the CHGVIEW command, or the execution of existing views.

If you plan to enable and use the *SEQUEL option it is imperative that you also consider the following:

- Users must not be allowed access to command entry. Command entry functions can always be used to view the contents of files based on standard system object authority.
- Users must be restricted from the Change View (CHGVIEW) command. Only the Sequel user interface (Viewpoint and green-screen) performs the additional security checks that you set up. You can restrict the CHGVIEW command by simply revoking operational authority to the command object.

For *SEQUEL with prompted views (object type SQLVIEWP), restrictions are enforced in the Viewpoint and green-screen view designers, for statements entered through command entry, in the CHGVIEW command, in the Script designer, and any 'Work with' screen (WRKSEQUEL, WRKVIEW, and the Viewpoint Explorer).

With *STRICT you get all the security of *SEQUEL. In addition, *STRICT applies equally to views with run-time variables and those without, and it applies at run time as well as design time. This option provides the strongest level of authority when used with any Sequel related feature or function.

Change the authority checking value back to *SYSTEM to return to system defined object checking. The user will be able to access the libraries and files to which they have operational and read authority. The exclusion/inclusion dictionary will be disabled but not cleared.

Since the type of authority checking to be done is kept in a user's default data area, the type of checking is user specific. If necessary, you can provide separate authority mechanisms for different users so that some users use *SYSTEM security and others use *SEQUEL or *STRICT authority.

You must ensure that Sequel users do not have administrative privileges (*CHANGE authority) to the SQ#DFT data area. Otherwise they will be able to use the SETDFT command to revert to *SYSTEM authority and enable themselves to objects you want protected. Users that should not change the defaults need only have *USE authority to the SQ#DFT data area.

Set User Option for Database Security

The Set User Option tab below provides an easy way to view and modify the object authority setting for multiple Sequel users. Leave the box empty for standard system object authority (*SYSTEM). Check the box next to a user to set their default for Object Authority Checking to *SEQUEL—the user's name will change to blue. Check the box a second time to set their default to *STRICT—the user's name will change to red. Check the box a third time to cycle back to *SYSTEM.

You can also access the <u>View Design Defaults</u> to change a user's Object Authority value, but you will probably prefer to use the display below.

Options

User Check Box - This change takes place instantly. Leave the box empty for standard system object authority (*SYSTEM). Check the box next to a user to set their default for Object Authority Checking to *SEQUEL—the user's name will change to blue. Check the box a second time to set their default to *STRICT—the user's name will change to red. Check the box a third time to cycle back to *SYSTEM.

Summary List Button   - Press the summary button to list users without any descriptive text.

Detail List Button   - Press the detail button to display the descriptive text for each user.

Apply Button - Press the Apply button to make changes to multiple users. Use Ctrl-click to select (or de-select) multiple users, or use Shift-click to select a range of users.

Close Button - Close the user list and return to the main Audit screen.

Menu Options:

File \ Close - Close the user list and return to the main Audit screen.

File \ Exit - Close the user list and completely exit Viewpoint Administrator.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

View Designer Interface Interaction

When a user enters the user interface (Viewpoint and green screen) after the Sequel security option is enabled, each field, file, and library reference is verified against the exclusion dictionary.

Items excluded from access will not appear in any prompt lists presented to the user. Thus, a generic or '*ALL' prompt request may return significantly fewer names than would otherwise be

observed using the same request outside of the user interface, or with the security option disabled.
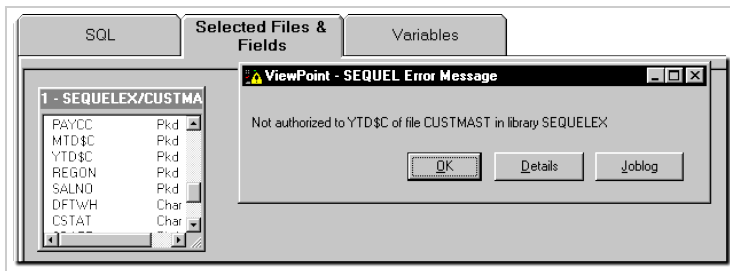
Fields that have been excluded from access cannot be specified directly or indirectly. Reference to an excluded field in the SELECT, WHERE, GROUP BY, HAVING, or ORDER BY clauses results in an error message at the workstation. The user must correct the error by removing the field reference before the query will run successfully. Calculations involving excluded fields are likewise disallowed.
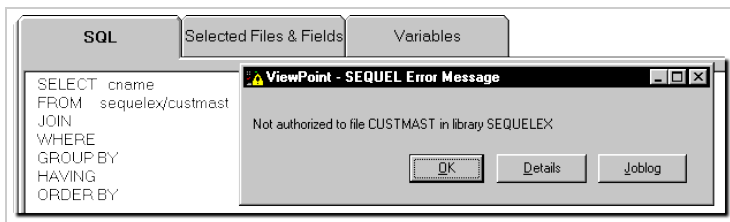
If any field level exclusion entries apply, the user interface will not allow the SELECT * form of the SELECT clause. Attempts to use SELECT * when one of the files has field level exclusion entries will result in an error message.
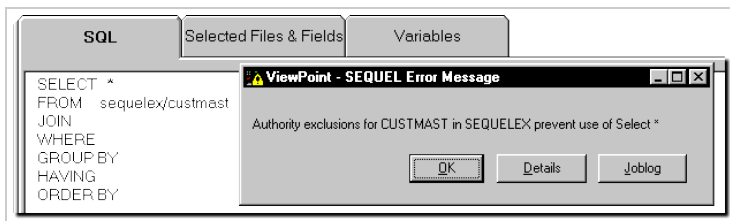
Setting Up the Exclusion Dictionary

Set Exclusions by Object

Use the Select by Object tab to take an object oriented approach to exclusion: first identifying objects (libraries, files and fields) that need to be excluded from user access, then selecting the users that must be excluded from accessing them. The display is divided into three sections: Library/File, Fields, and User Profile.

Use the Select by User tab to change the display and set exclusions by user.

Use the Set User Option to set a user's default to use the exclusion dictionary.
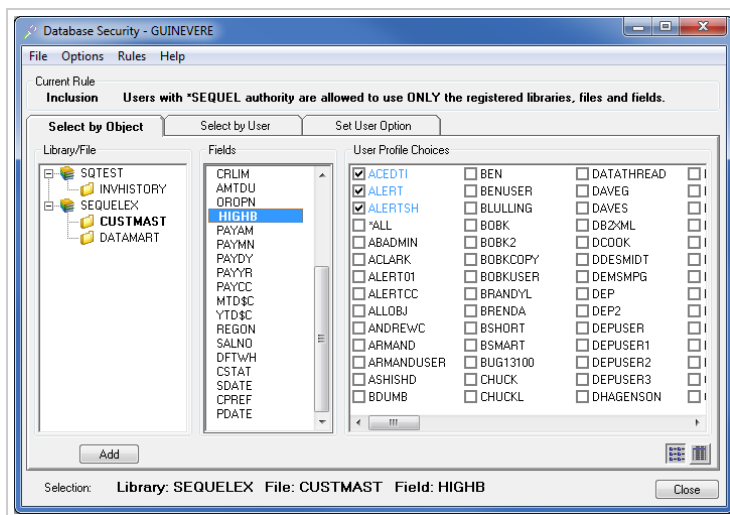
Options

Library/File Pane - All library and file objects currently represented in the exclusion dictionary are show in this pane. Click the [+] to expand the library to see the files. Select a file to see the fields listed in the Fields pane. New library and file entries can be added using the Add button or by right clicking in the pane and using the available menu.

Add Button - Press the add button to add files for a given library. The Select Files dialog will allow you to search for files to add to the exclusion dictionary.

Fields Pane - Select a file to see the fields in the Fields pane. Any fields that have exclusions will be listed in blue. The value *ALL is used to exclude all fields in the file.

User Profiles Pane - Users that are excluded from a given object will be shown first in the list in blue and with a check next to their name. Uncheck them to allow them to use the object. To exclude a user place a check next the their name and press the Refresh button.

Summary List Button ⊞ - Press the summary button to list users without any descriptive text.

Detail List Button ▦ - Press the detail button to display the descriptive text for each user.

Close Button - Close the user list and return to the main Administrator screen.

Menu Options

File \ Close - Close the user list and return to the main Administrator screen.

File \ Exit - Close the user list and completely exit Viewpoint Administrator.

Options \ Refresh - Refresh the list of files.

Options \ Expand All - Expand the list of libraries and files.

Options \ Collapse All - Collapse the list of libraries and files.

Rules \ Exclusion - Change the dictionary from inclusion to exclusion.

Rules \ Inclusion - Change the dictionary from exclusion to inclusion.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Set Exclusions by User

Use the Select by User tab to take a user oriented approach to exclusion: first identifying users that need to be prevented from accessing objects (libraries, files and fields) then selecting the objects that need to be secured. The display is divided into three sections: User Profile, Library/File, and Fields.

Use the Select by Object tab to change the display and set exclusions by object.

Use the Set User Option to set the user's default to use the exclusion dictionary.
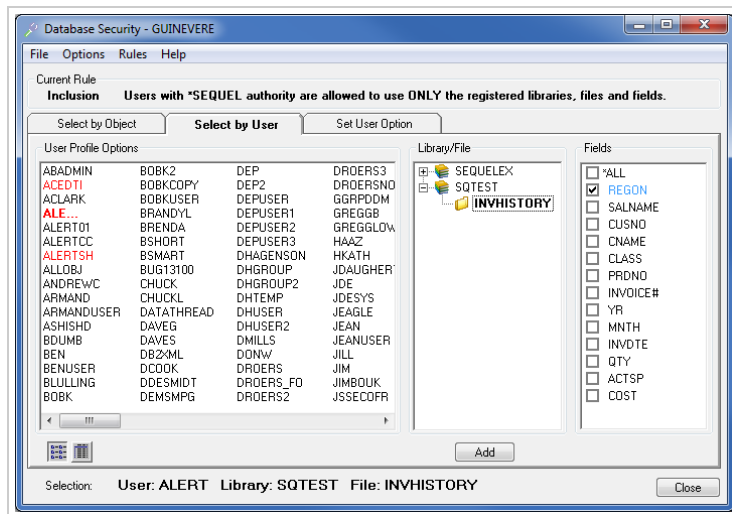
Options

User Profiles Pane - Select the user you want to work with.

Library/File Pane - If the selected user has exclusions defined, you will see libraries and files listed. Click the [+] to expand the library to see the files. Select a file to see the fields listed in the Fields pane. New library and file entries can be added using the Add button or by right clicking in the pane and using the available menu.

Add Button - Press the add button to add files for a given library. The Select Files dialog will allow you to search for files to add to the exclusion dictionary.

Fields Pane - Select a file to see the fields in the Fields pane. Any fields that have exclusions will be listed in blue. The value *ALL is used to exclude all fields in the file.

Summary List Button [icon] - Press the summary button to list users without any descriptive text.

Detail List Button [icon] - Press the detail button to display the descriptive text for each user.

Close Button - Close the user list and return to the main Administrator screen.

Menu Options

same as the *Menu Options* on page 70

Adding and Removing Libraries

To add a library, right-click a current library and choose **Add File to Library XXX**. This will take you to the Select Files Screen. You can also press the Add button.
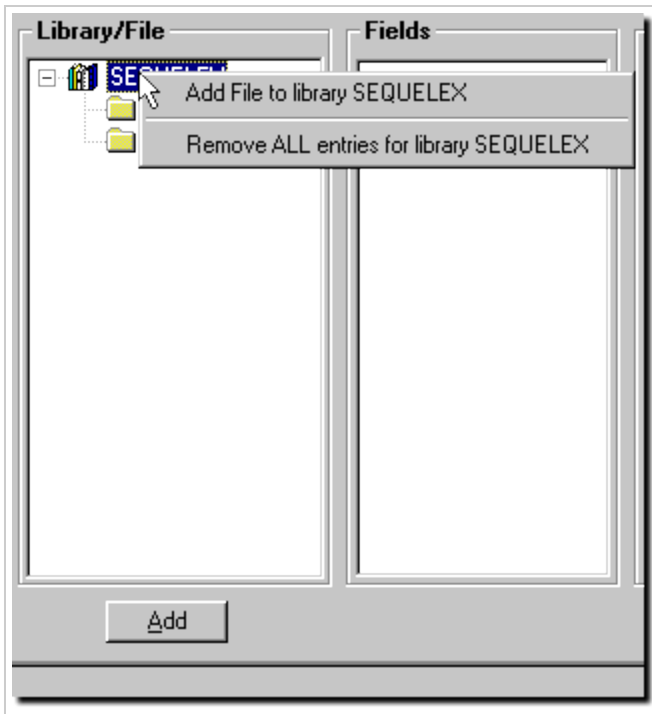
To remove a library, right-click and select Remove all entries for Library XXXX.

Adding and Removing Files

To add a file, right-click a current library and choose **Add File to Library XXX**. This will take you to the Select Files Screen. You can also press the Add button.
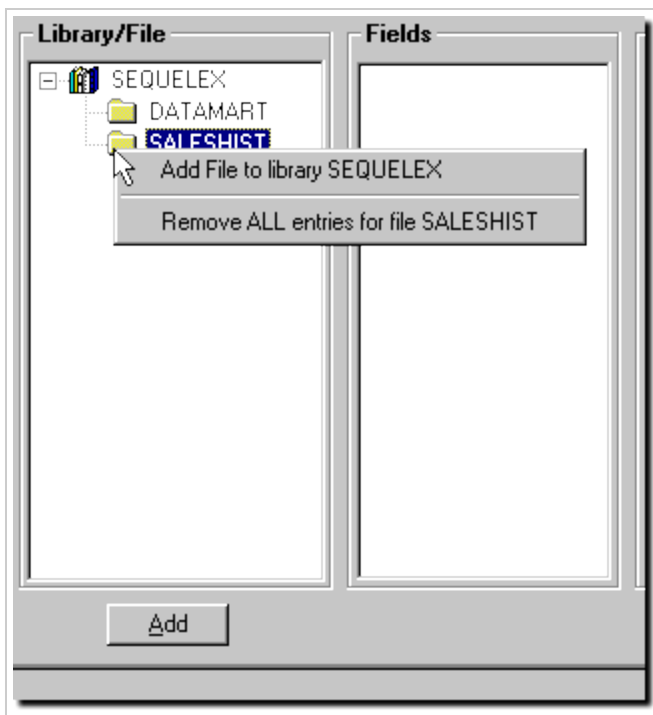
To remove a file, right-click and select Remove all entries for file XXXX.

Select Files

The select files dialog is accessed when setting exclusions by object or user, or when adding or removing libraries or files to the exclusion/inclusion dictionary.

Use this screen to choose a library and a file from that library.
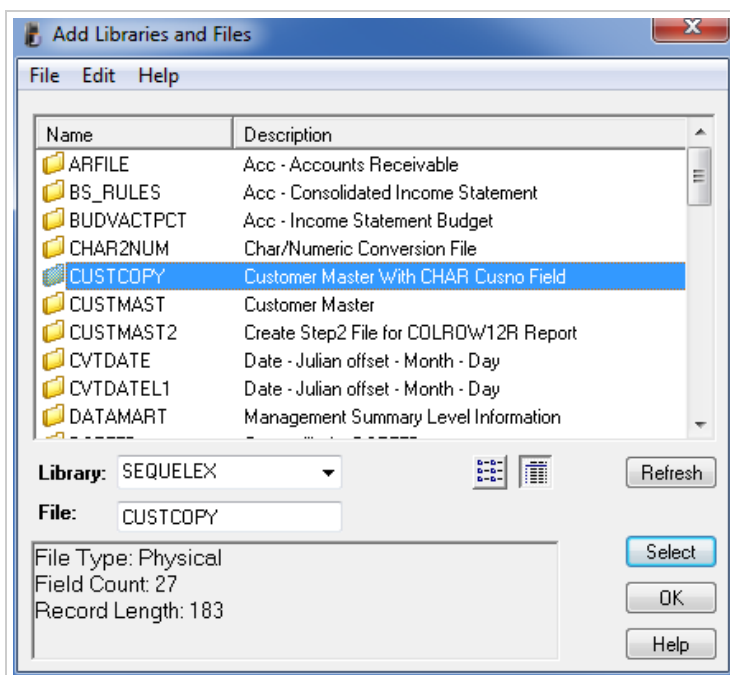
Options

Menu Options:

File \ Close - Close the user list and return to the Field Level Authorization screen.

File \ Exit - -Close the Select File display and completely exit Viewpoint Administrator.

Edit \ Refresh - Refresh the list of files.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Screen Elements:

Library - Enter a library name, or choose one of the special values from the drop down menu.

File - Displays the selected file, or you can enter a file name.

Summary List Button - Press the summary button to list files without any descriptive text.

Detail List Button - Press the detail button to display the descriptive text for each file.

Refresh Button - Press the Refresh button after specifying a new library to see the files in that library.

Select Button - Press the Select button after highlighting a file.

Close Button - Press to close the Select Files dialog.

Help Button - Press to open the on-line help system.

How to Exclude an Entire Library

Use one of the two processes below to set an exclusion to an entire library.

Object Oriented: (Select by Object)

1. In the Library/File pane, highlight the **library** you want to exclude.
   Use the **Add** button if you need to add a library to the list.

2. In the Fields pane highlight the entry *****ALL**.

3. Select the user(s) you want to exclude from the library.
   You can select *ALL to exclude all users from the library.
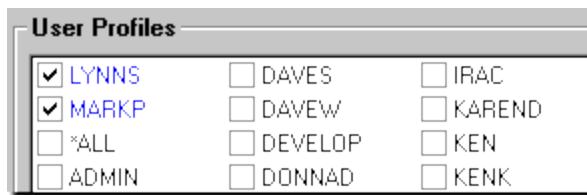
Press the **Refresh** button to see the changes.

User Oriented: (Select by User)

1. In the User Profile pane, select the **user** you want to define exclusions for.
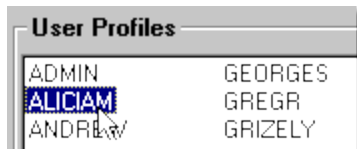
2. In the Library/File pane, highlight the **library** you want to exclude.
   Use the **Add** button if you need to add a library to the list.
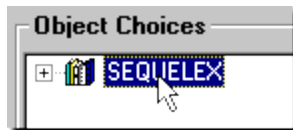
3. Select ***ALL** in the Fields pane.
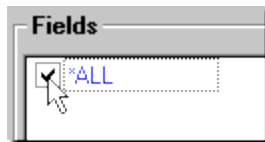
How to Exclude an Entire File

Use one of the two processes below to set an exclusion to an entire file.

Object Oriented: (Select by Object)

1. In the Library/File pane, click the [+] to expand the library and highlight the **file** you want to exclude.
   Use the **Add** button if you need to add a file to the list.
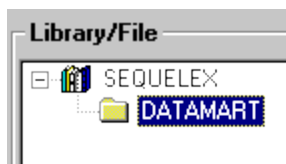
2. In the Fields pane highlight the entry ***ALL**.
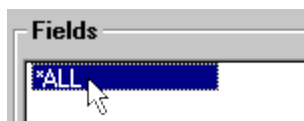
3. Select the **user(s)** you want to exclude from the file.

You can select *****ALL** to exclude all users from the file.
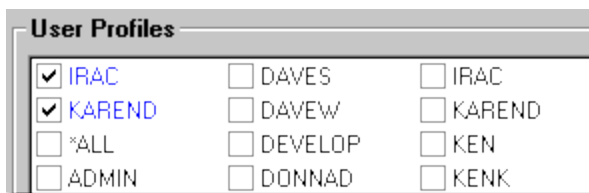
Press the **Refresh** button to see the changes.

User Oriented: (Select by User)

1. In the User Profile pane, select the **user** you want to define exclusions for.
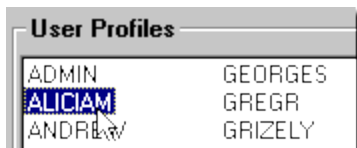
2. In the Library/File pane, click the [+] to expand the library and highlight the **file** you want to exclude.

    Use the **Add** button if you need to add a file to the list.
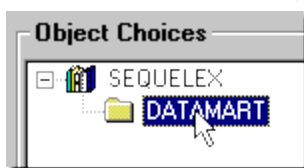
3. Select *****ALL** in the Fields pane.
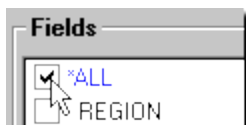
How to Exclude Fields

Use one of the two processes below to set and exclusion to one or more individual fields.

Object Oriented: (Select by Object)

1. In the Library/File pane, click the [+] to expand the library and highlight the **file** you want to work with.

    Use the **Add** button if you need to add a file to the list.
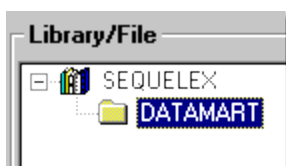
2. In the Fields pane highlight any of the **fields** listed.
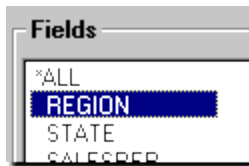
3. Select the **user(s)** you want to exclude from the field.

   You can select *****ALL** to exclude all users from the field.
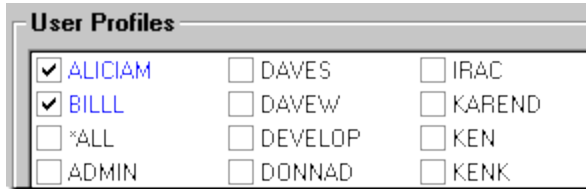
   Press the **Refresh** button to see the changes.

User Oriented: (Select by User)

1. In the User Profile pane, select the **user** you want to define exclusions for.
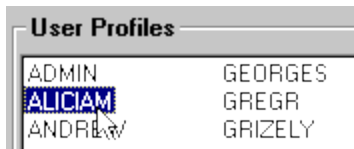
2. In the Library/File pane, click the [+] to expand the library and highlight the **file** you want to work with.

   Use the **Add** button if you need to add a file to the list.
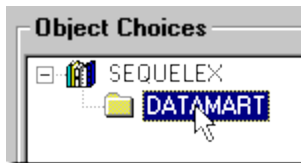
3. In the Fields pane, place check marks next to the **field(s)** you want excluded.
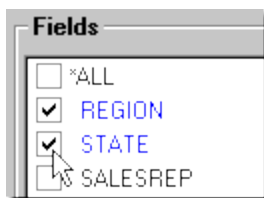
Advanced Database Security

About Advanced Database Security

Much like the Database Security feature, the Advanced Database Security (ADS) feature allows administrators to apply security to host libraries, tables, and columns. The major difference between the two security options is the ability to apply row level security to tables. These multiple levels of security can be based on group (primary or supplemental), user, and *PUBLIC profiles.

ADS requires the configuration and use of the Viewpoint Universal Driver to connect to the host when using Viewpoint. Users are forced to use this connection which enforces the rules defined in ADS.

In addition, several global server-level options can applied to control things such as excluding users from all files or libraries, and limiting *ALLOBJ profiles.

Column Security

Column security allows users to see the data in some columns of a database file, while restricting them from seeing data in other columns. For example, an employee master file might contain employees' names, titles, department numbers, hire dates, and social security numbers. Some of your users may need access to the information, but you want to keep the social security numbers confidential. By applying column security, you can exclude all users or specific users from seeing the social security column, while allowing them to access all other columns.

Without column security, you would not be able to restrict users from any of the data in files that contain columns with sensitive information. Column security gives you much more flexibility in deciding which files your users may access.

Row Security

Row security allows users to see the data in some rows of a database file while restricting them from seeing data in other rows. For example, a prospective customer file might contain prospect information for your company's potential clients around the world. However, you only want the sales managers in each country to be able to view information about prospects in their own country. Using row security, you can exclude users from seeing the rows that contain information about prospects in other countries.

Without row security, you would not be able to allow users access to any of the data in files that contain rows with information they should not see. Row security gives you much more flexibility in deciding which files your users may access. ADS gives you a way to specify this row security through a graphical user interface, without forcing you to write user exit programs.

When applying row security, using the example above, you would first ensure that each sales manager had access to the prospect file. For the U.S. sales manager, create a row condition similar to <COUNTRY>='USA', where <COUNTRY> is the name of the column containing country information and choose that person's user profile for the rule. Then, you would create another rule--<COUNTRY>='DEU' and apply this to the German sales manager. Repeat this for the sales manager in each country.

The Advanced Database Security Interface

The Advanced Database Security (ADS) interface is divided into three functional tabbed areas.

Use the Select by Object tab to create rules and assign them to users and groups. This tab is divided further into three sections: Library/File/Fields, Rules, and User Profile Choices. Use the Select by User tab to review the rules that are currently applied to users. Use the Server Options tab to set system-wide global security settings.
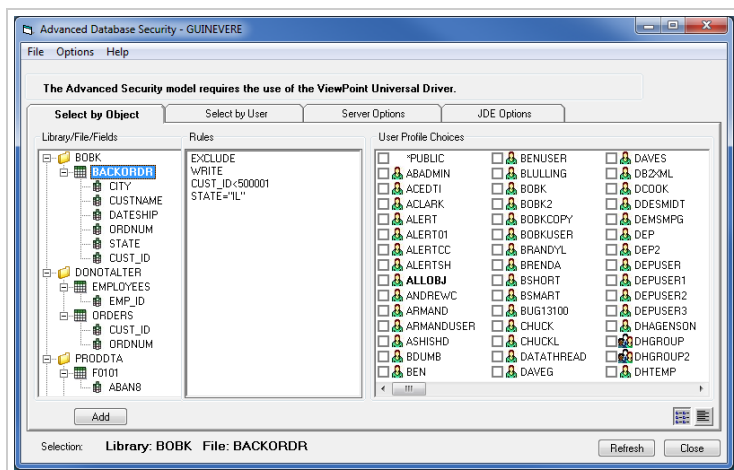
Options

Library/File/Fields Pane - All library, file, and field objects with existing rules are shown in this pane. Click the [+] to expand the library to see the files. Select any item in the list to see the rules listed in the Rules pane. New rules can be added using the Add button or by right-clicking any item in the pane and using the add option.

Add Button - Press the Add button to add rules. Use the ADS Rules screen that displays to search for libraries, files or fields for the new rule.

Rules Pane - Any rule associated with a selected item in Library/File/Fields pane is displayed here. Select a rule to see the assigned users in the User Profile pane. Assigned users are listed in blue at the beginning of the list. The value *PUBLIC, when checked, indicates the rule is applied to all users.

User Profile Choices Pane - Users assigned to a selected rule are shown first in the list in blue and with a check next to their name. Uncheck a user or group to remove from the rule. Add additional users to a selected rule by placing a check next to their name. Use the Refresh button to update the list.

Summary List Button - Press to list users without any descriptive text.

Detail List Button - Press to display the descriptive text for each user.

Refresh Button - Press to refresh the displayed data.

Close Button - Close the user list and return to the main Administrator screen.

Menu Options

File \ Close - Close the ADS display and return to the main Administrator screen.

File \ Exit - Close the ADS Display and completely exit Viewpoint Administrator.

Options \ Refresh - Refresh the ADS database and displayses.

Options \ Expand All - Expand the list of libraries and files.

Options \ Collapse All - Collapse the list of libraries and files.

Help \ Contents -Open the on line help.

Help \ About - Display Administrator version information.

Adding Rules

The work flow for creating ADS rules is very simple: Define a rule for a library, file, field, or row, and then apply it to a user, group, or all users. The process and screens used change slightly depending on the type of rule you wish to create.

By Library

1. Starting at the Select by User Tab, right-click on an existing library and select **Add**.
   You can also press the Add button at the bottom of the screen.
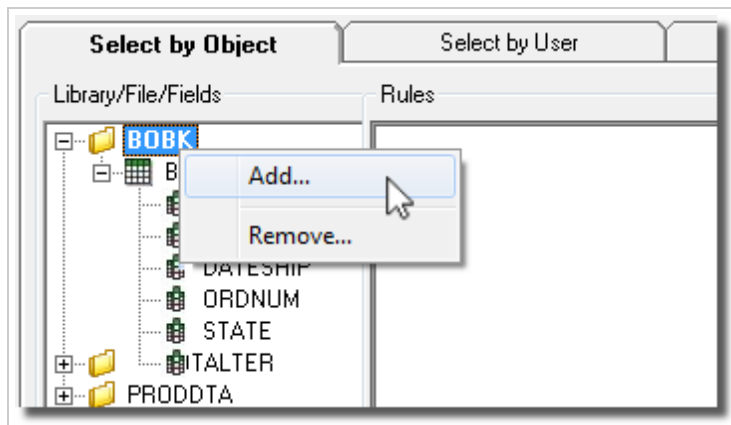
2. In the Security Rules display, the current library is listed. Use the **Browse** button to select a new library, or type in a library name.
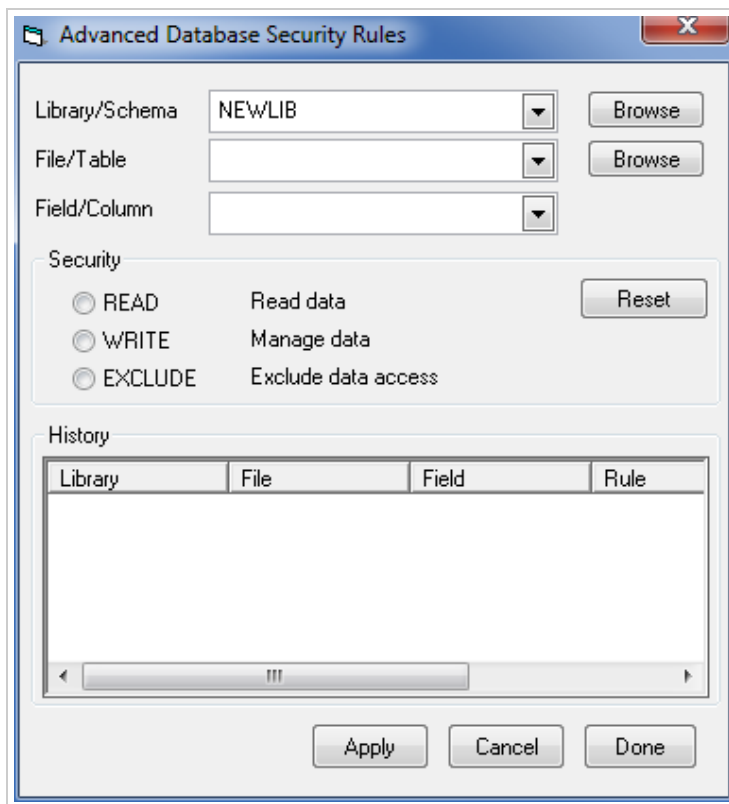
3. Select one of the three security options listed:

> **Read** - The assigned user is allowed to read data from any unrestricted file in this library.

> **Write** - Not enforced at this time.

> **Exclude** - The assigned user is restricted from every file in the library.

4. Press one of the following buttons:

> Press **Reset** to clear your selection and select a different value. Use Reset before the Apply button or you must delete the rule from the main screen.

> Press **Apply** and your rule will display in the History panel. Because you can continue defining rules for libraries and files (before pressing the Done button), this panel helps you keep track of your rules as you create them.

> Press **Done** to exit this screen and write your rule(s) to the ADS database.

5. Back at the main screen you should see your new rule displayed in the Library/Files/Fields tree. Select it and then select the rule in the Rules list.
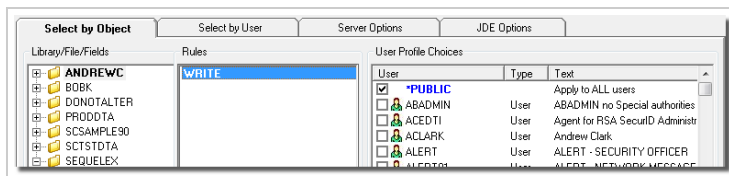
6. Notice *PUBLIC is selected by default as the user. This is done to ensure no new rule is created without an assigned user in the ADS database. If you want to apply the new rule to all users, leave *PUBLIC as is. Otherwise, select specific users for which to assign the rule.

By File

The steps to define a file-based rule are almost exactly the same as the library rule described above. At step 2, use the file Browse button to select a file and continue with the remaining steps.

By Field

1. Starting at the Select by User Tab, right-click on an existing field and select **Add**. You can also press the Add button at the bottom of the screen.
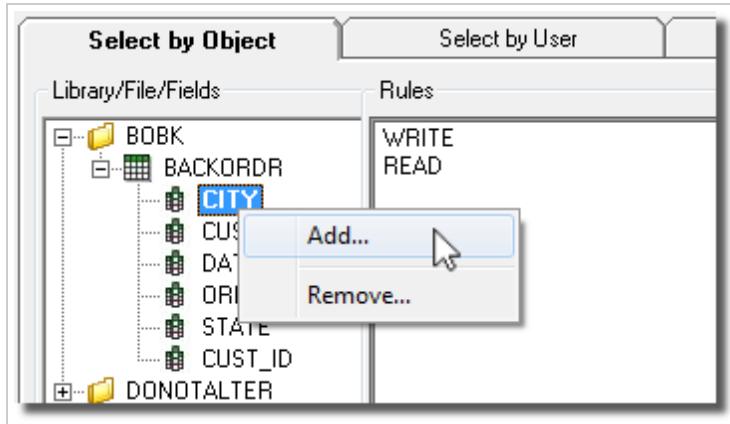
2. In the Security Rules display, the current library and file is listed. Use the **Browse** buttons to select a new library or file.
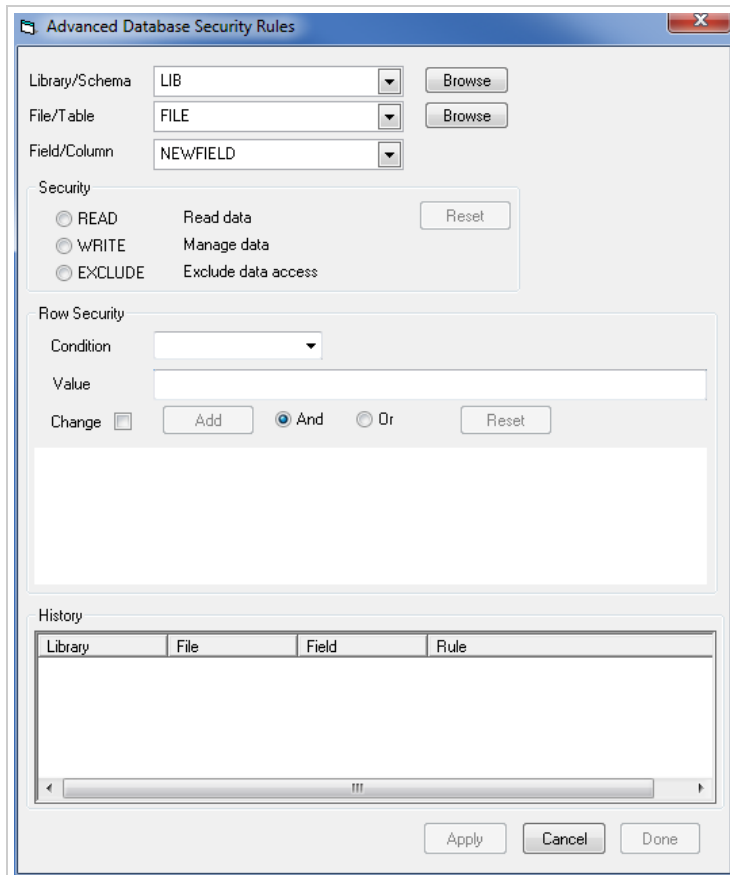
3. Use the Field/Column drop-down to select a field.
4. Select one of the three security options listed:

> **Read** - The assigned user is allowed to read data from any unrestricted file in this library.
>
> **Write** - Not enforced at this time.
>
> **Exclude** - The assigned user is restricted from every file in the library.

5. Press one of the following buttons:

> Press **Reset** to clear your selection and select a different value. Use Reset before the Apply button or you must delete the rule from the main screen.
>
> Press **Apply** and your rule will display in the History panel. Because you can continue defining rules for libraries and files (before pressing the Done button), this panel helps you keep track of your rules as you create them.
>
> Press **Done** to exit this screen and write your rule(s) to the ADS database.

6. Back at the main screen you should see your new rule displayed in the Library/Files/Fields tree. Select it and then select the rule in the Rules list.

7. Notice *PUBLIC is selected by default as the user. This is done to ensure no new rule is created without an assigned user in the ADS database. If you want to apply the new rule to all users, leave *PUBLIC as is. Otherwise, select specific users for which to assign the rule.

By Row

A row-based rule can be a little confusing because it is defined by specifying a field and a filter to restrict or allow file access at the row level. So a row rule is in essence, a file rule. Also, the rule is built like an SQL WHERE clause. So, if you want to use a condition on a single field to specify multiple values, do this:

```
REGION = 10 or REGION = 20
or:
REGION IN (10, 20)
not:
REGION = 10 AND REGION = 20
```
(this will not return any records)

The process to create a row-based rule is very similar to the field process above with the addition of the Row Security section.

1. Starting at the Select by User Tab, right-click on an existing field and select Add. You can also press the Add button at the bottom of the screen.
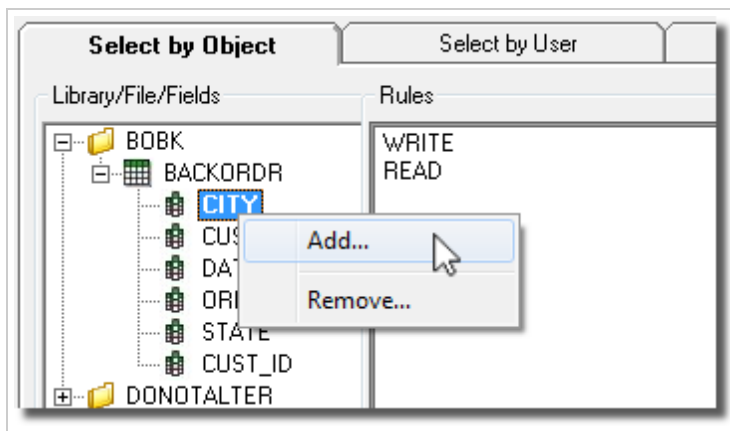
2. In the Security Rules display, the current library and file is listed. Use the Browse buttons to select a new library or file.
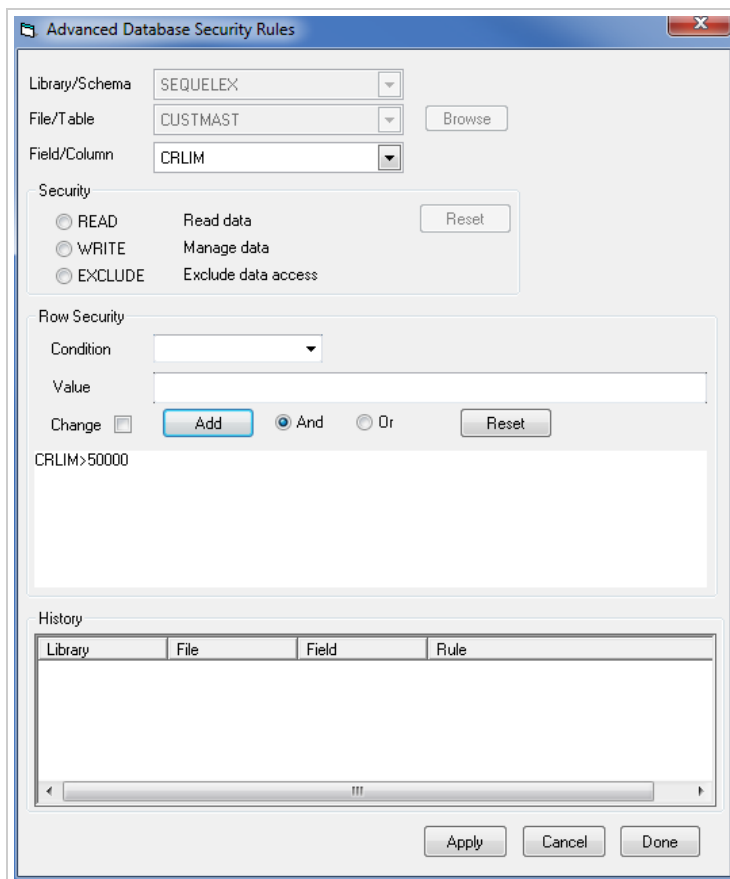
3. Use the Field/Column drop-down to select a field.
4. In the Row Security section set the following:

> > **Condition** - Use the drop-down to select a condition.
>
> > **Value** - Enter the value to filter records based on the selected field and field type. Make sure to use quotes for character data.
>
> > **Change** - Check this box to modify existing expressions. See the Modifying Rules topic below.
>
> > **Add** - Press to create the rule.
>
> > **And / Or** - To create complex conditions, select AND or OR and then build another expression.

5. Press one of the following buttons:

    > Press **Reset** to clear your expression(s). Use Reset before the Apply button or you must delete the rule from the main screen.

    > Press **Apply** and your rule will display in the History panel. Because you can continue defining rules for libraries, files, and rows (before pressing the Done button), this panel helps you keep track of your rules as you create them.

    > Press **Done** to exit this screen and write your rule(s) to the ADS database.

6. Back at the main screen you should see your new rule displayed in the Library/Files/Fields tree. Select it and then select the rule in the Rules list.
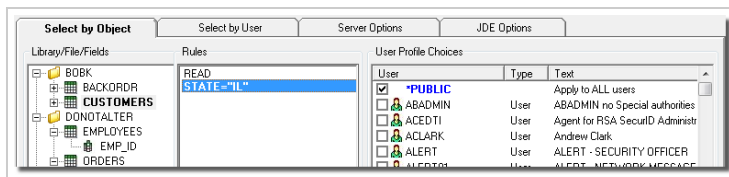
7. Notice *PUBLIC is selected by default as the user. This is done to ensure no new rule is created without an assigned user in the ADS database. If you want to apply the new rule to all users, leave *PUBLIC as is. Otherwise, select specific users for which to assign the rule.

Modifying Rules

Library, File, or Field

1. To modify existing rules, start in the Select by Object panel and highlight a library, file or field.

2. Double-click the WRITE, READ, or EXCLUDE rule listed in the Rules pane.
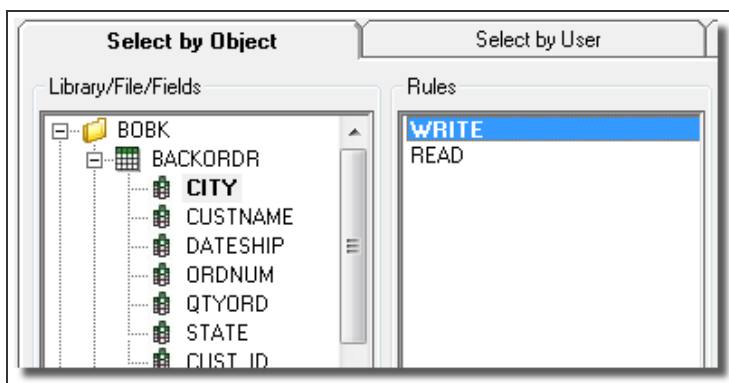
For a library, file, or field rule the Security Rules screen shows the object associated with the rule (grayed out) and the current value.
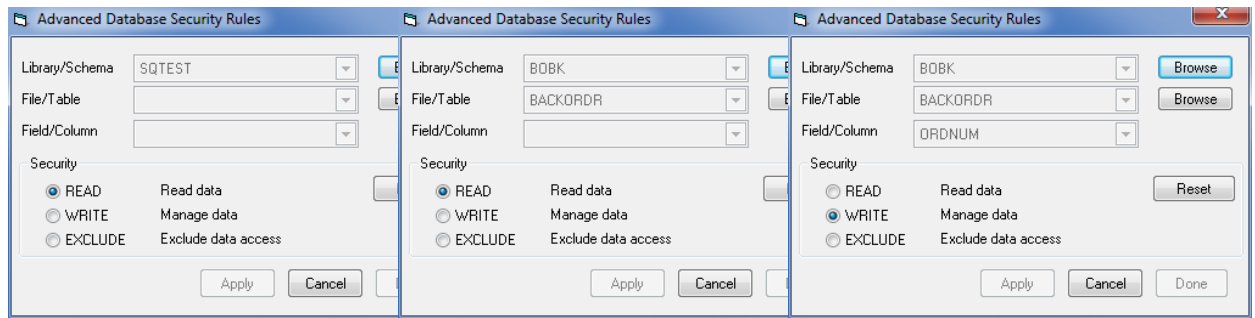
Modify Library   *Modify File*   *Modify Field*

3. Simply choose a different value and press the **Apply** button.

Row

1. Start in the Select by Object pane and highlight a field that has row-based rules.
2. Double-click the filter rule listed in the Rules panel.
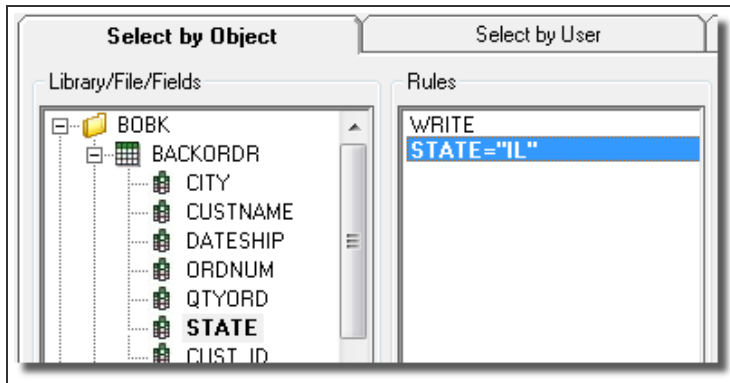
For row-based rules, the Security Rules screen is different than the three shown above. Notice only the library and file are grayed out. This allows for adding additional expressions to a rule, or changing the current expression.
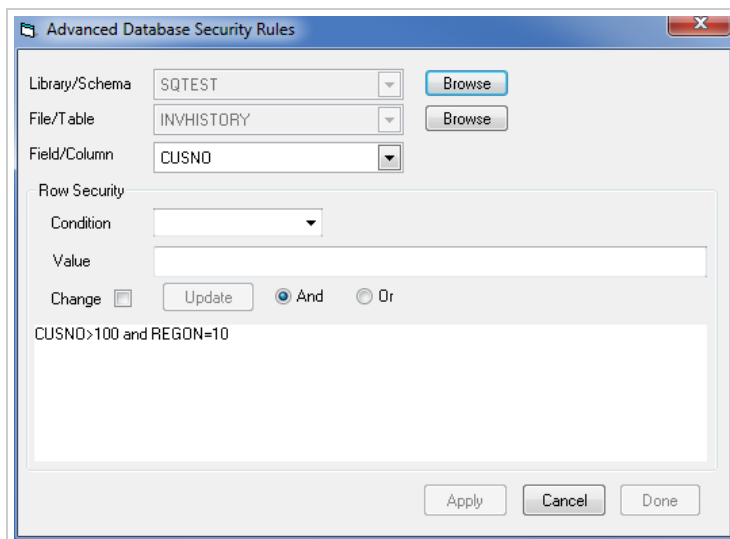
Add to an Expression

1. To add to the current expression, select a field, condition, and value.
2. Then select AND or OR and press the **Update** button.

3. The additional expression is added to the current expression.

4. Press **Apply** to save your change and close the window.

Change the Expression

1. To change the current expression, or part of one, place a check in the change box.

    This will separate complex expressions into multiple lines so you can work with each individually.

2. Double-click and expression and it will fill in the Field, Condition and Value fields.

3. You can select a different field, change the condition, and change the value. Here, the value was changed from 10 to 50.
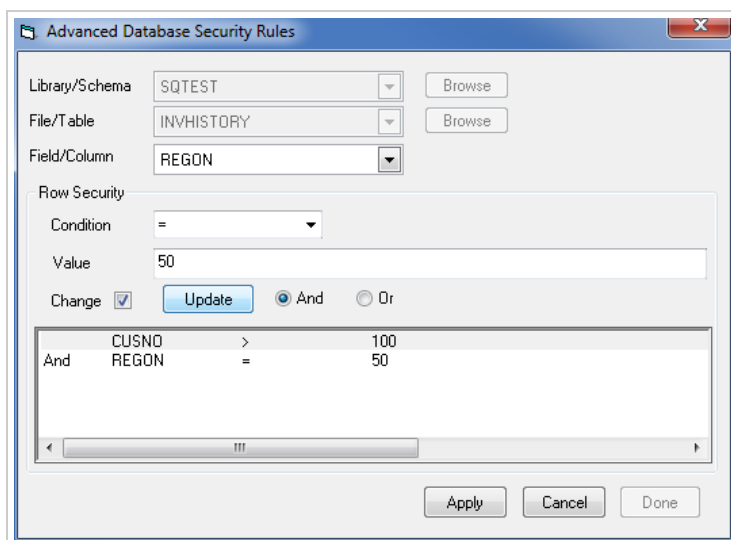
4. Press **Update** to see the change followed by **Apply** to save the change and close the display.

Reviewing Rules

The Select by User tab is a great way to see who has rules applied. In the User Profile Options panel, users, groups, or *PUBLIC will be blue and bold if they have any rule applied. The Library/File/Fields pane shows any object currently referenced in a rule. The Rules pane is blank until a rule is selected.
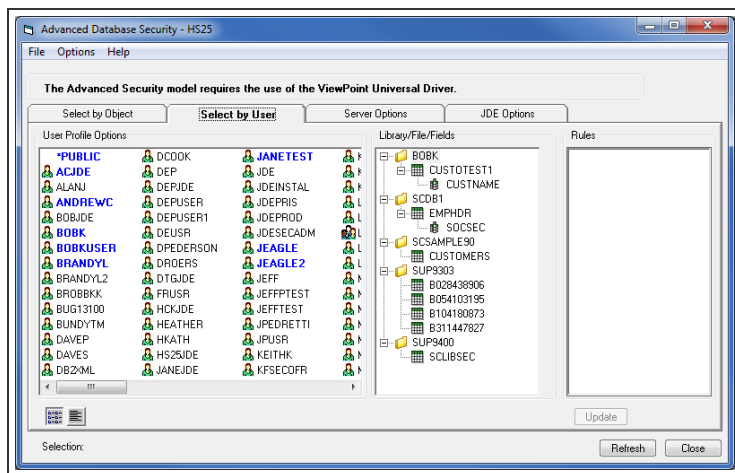
To see the exact rule for a user, group, or *PUBLIC, select the user. Any object referenced by a rule for the user will display as blue in the Library/File/Fields pane. Select the object to see the definition in the Rules pane.

In the example below, we see user BOBKUSER is excluded from the CUSTNAME field in the CUSTOTEST1 file.
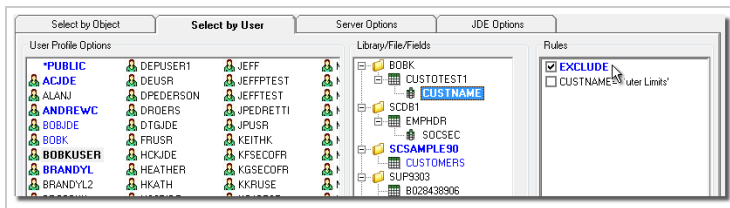
You can deselect the rule to remove the limitation for the selected user. You can also apply any of the existing rules to the selected user by selecting any other item in the Library/File/Fields pane (one that is not blue), and apply its defined rule.

In this example, BOBKUSER is still selected, and by clicking on the SOSEC field in the EMPHDR file, we see there is an EXCLUDE rule already defined for some other user. Simply check the rule to apply it also to BOBKUSER. Press **Refresh** to see the change.
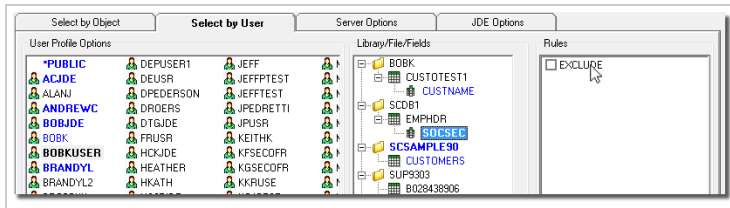
Server Options

The Server Options tab allows for easy application of system-wide, or global, defaults that are automatically applied to all users when using Viewpoint in conjunction with the Viewpoint Universal Driver.

Set global options to:

- Exclude user from viewing all libraries by default.
- Exclude users from viewing all files by default.
- Apply security to supplemental groups.
- Load Security information on startupl.
- Enforce Advanced Database security even on users with *ALLOBJ authority.
- Display all libraries or just the user's library list.
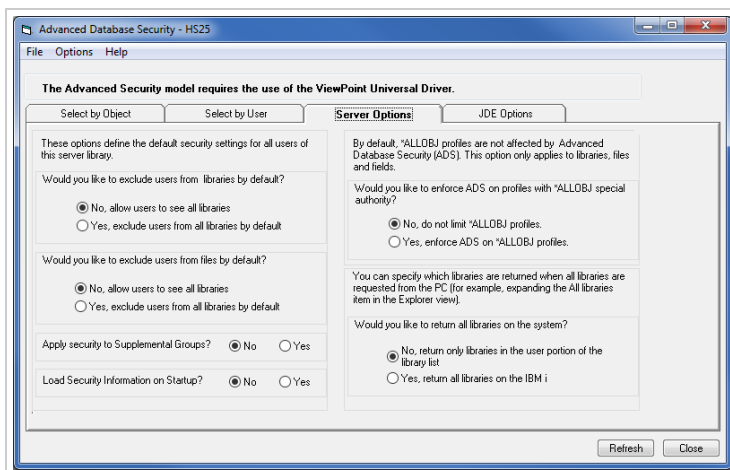
Options

The following settings are optional and are set when the host is installed.

Exclude users from libraries by default.

No (default) - Users are allowed to access all libraries. Users can be excluded from specific libraries.

Yes - Users are excluded from accessing all libraries. Users must be granted access to specific libraries.

Exclude users from files by default.

No (default) - Users are allowed to access all files. Users can be excluded from specific files.

Yes - Users are excluded from accessing all files, and must be granted access to specific files.

Apply security to supplemental groups.

No (default) – Supplemental Group memberships will be ignored (primary groups are still honored)

Yes - Security will be applied to both Supplemental Groups and primary groups

Load Security Information on Demand

Yes (default) – Loads security information as needed. This improves performance.

No – Loads all security information when a user connects.

Enforce ADS on profiles with *ALLOBJ special authority.

No (default) - Showcase Securities are not applicable on *ALLOBJ User profiles

Yes - Showcase Securities are enforced on *ALLOBJ User profiles

Return all libraries on the system.

Yes (default) - Returns all libraries on the IBM i machine

No - Returns only libraries in the user portion of the library list

JDE Options

Use this tab to alter ADS settings specific to JD Edwards users access to all libraries vs. their user library list.
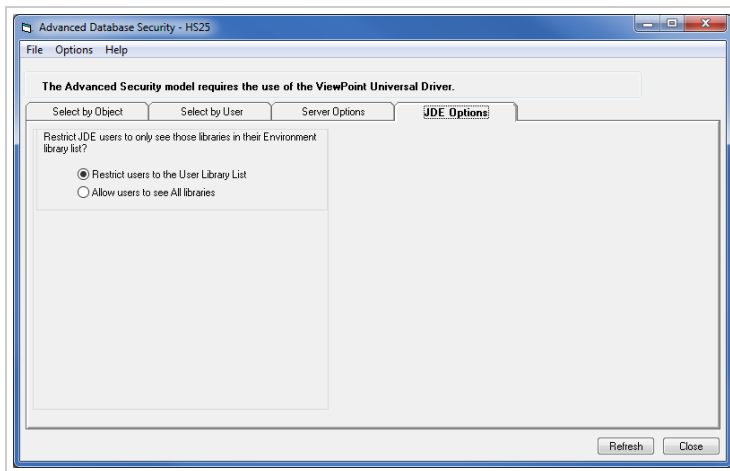
Enforcing Rules

The rules created and added to the ADS database are used and recognized only by the Viewpoint Universal Driver. To enforce the rules you must create a connection with the driver, and set user's Sequel defaults to use only the copied host file and the new connection. Everything the user does in Viewpoint is checked against the ADS database to apply the rules defined for that user, group, or all users. Follow the steps in the next five sections to accomplish this:

Copy the IBM i Driver

Before creating a new host connection, it is necessary to copy the IBM i driver into the correct directory so that the ADS connection can use it. Issue the following command from an IBM I command line:

```
CPY OBJ('/qibm/proddata/http/public/jt400/lib/jt400.jar') TODIR
('/rio/lib')
```

Copy the Host File

SequelHOST is the default host file shipped with the product.You can make multiple copies of the host file and tailor it to your environment so that each department or work group can have their own set of data sources or to ensure ADS users only have the ADS connection available to them.

1. Open Viewpoint Administrator and select your system, check the **Maintain Host Servers** option, and press **OK**.
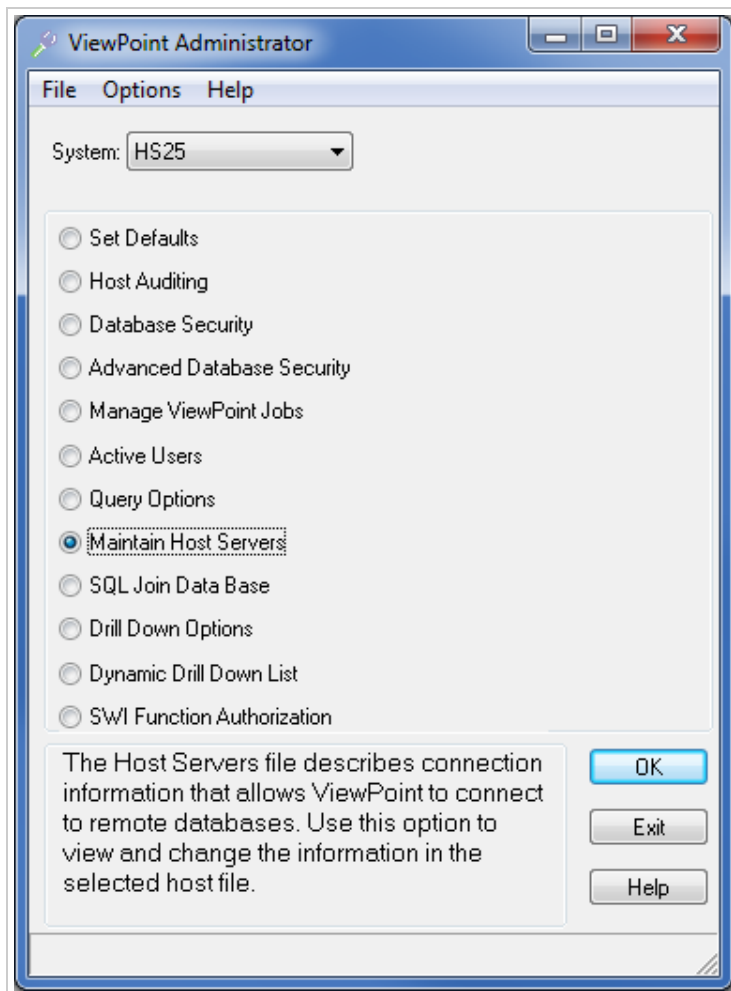
2. When the Host List screen opens, select **File\New** from the menu. In the New Host File dialog, give your new file a name and library and press OK. Do not create a file with the same name as the original SequelHOST file.
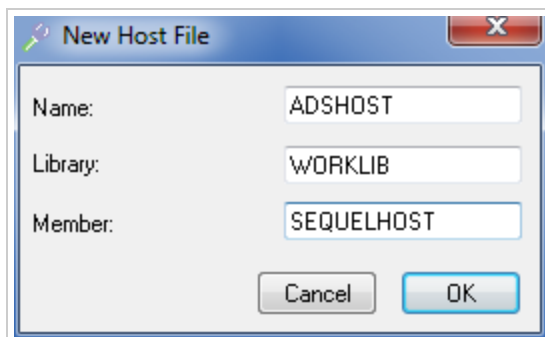
If you prefer the command line, issue the following:

```
CRTDUPOBJ OBJ(SEQUELHOST) FROMLIB
(SEQUELSCSERVER10) OBJTYPE(*FILE)
TOLIB(WORKLIB) NEWOBJ(ADSHOST) DATA(*YES)
```

> The new file is placed in the library specified by the TOLIB parameter.

Back at the Host List you should see the new host file and library at the top of the screen. Leave the Host List screen open for the next step of the process.

Create a Host Connection

Host connections are created so you can connect to non-DB2 databases (SQL Server, Oracle, MySQL, JDE World, and JDE Enterprise One), and now to connect locally to enforce ADS settings. These connection definitions will be stored in the copy of the host file created in the previous steps above.

1. Right-click in the Server panel and select **Add New Server Entry**.
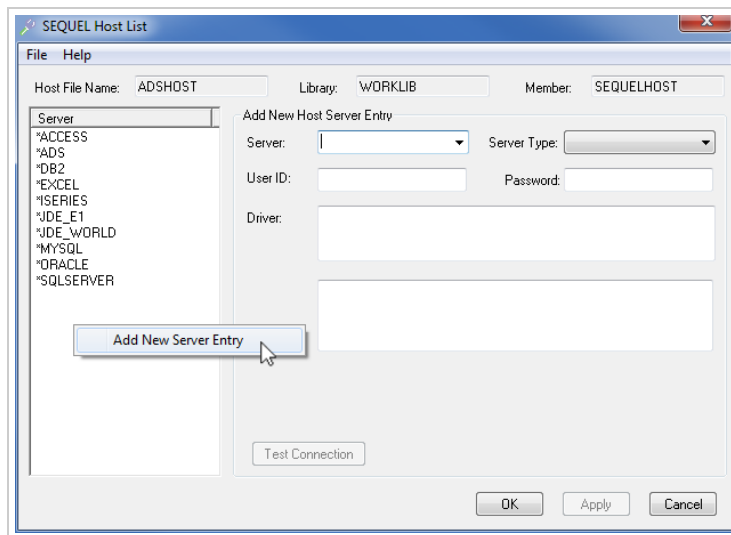
2. Set the following values:

   Server = NEWCONNECTION (or a name of your choice). Do not use an asterisk (*) in the name.

   Server Type = Select *ADS from the drop-down.

   Connection = Enter the following:

   jdbc:hslocal://<HOST_NAME>;installDir=<DRIVER_JAR_LOCATION>;installLib=<HOST_SOFTWARE>;

   where
   <HOST_NAME> = The name of the host System i machine. This value is mandatory.

   <DRIVER_JAR_LOCATION> = IFS path where the driver jar and configuration file is placed. The default path is /rio/lib. This value is mandatory.

   <HOST_SOFTWARE> = Location of Sequel 10 on the System i. The default is SEQUEL.

3. Press **Apply** to add the connection to the list.
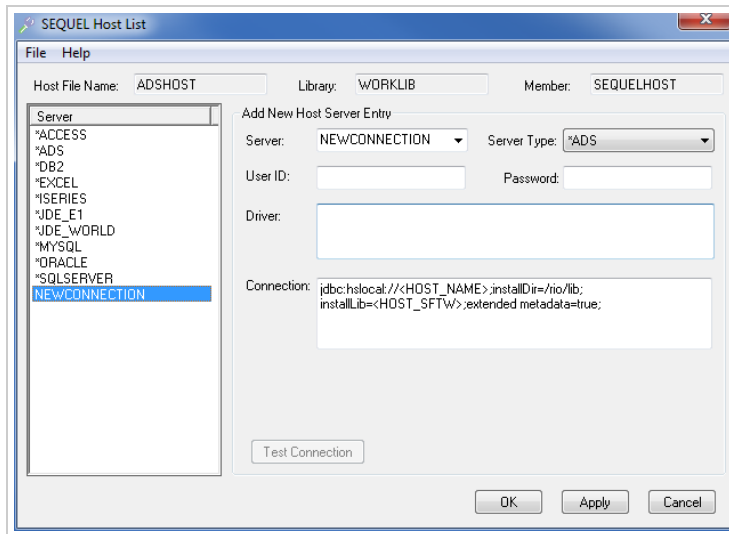
4. Press **OK** to close the window.

Set User Defaults

1. Back at the Administrator main menu, select Set Defaults and press OK.
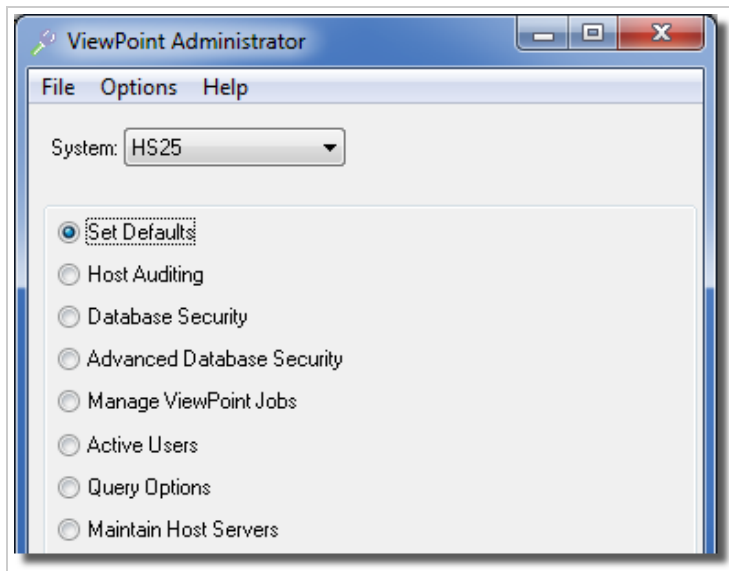
2. In the Defaults Selection screen, double-click a user to work with their defaults.
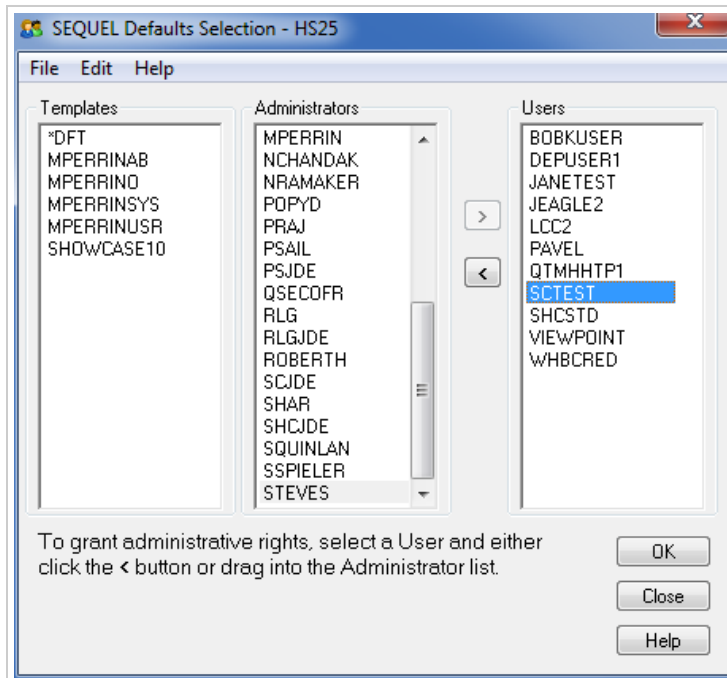
3. Open the Host tab and set the following:
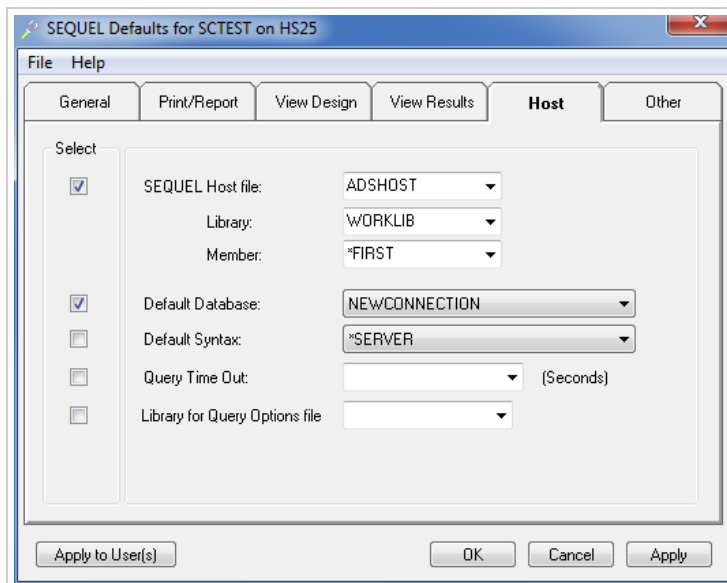
Host File = ADSHOST (or the name of the copied file)

Library = The library for the copied file.

Default Database = NEWCONNECTION (or the name you gave the new connection)

4. Open the **View Design** tab and set the **Object Authority Checking** default to ***ADS**.
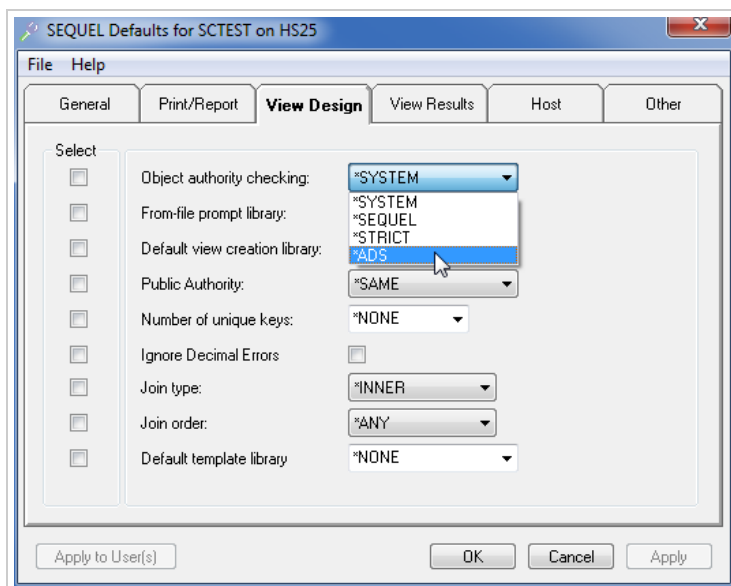
5. If you want to apply these setting to only the user you started with, press OK, and OK again at Defaults Selection screen.

6. To apply the settings to multiple users, check the box to the left of the Host File and Default Database defaults on the Host tab, and Object Authority Checking default on the View Design tab, and then press **Apply to User(s)**.

7. Check the users for the new settings and press **OK**.
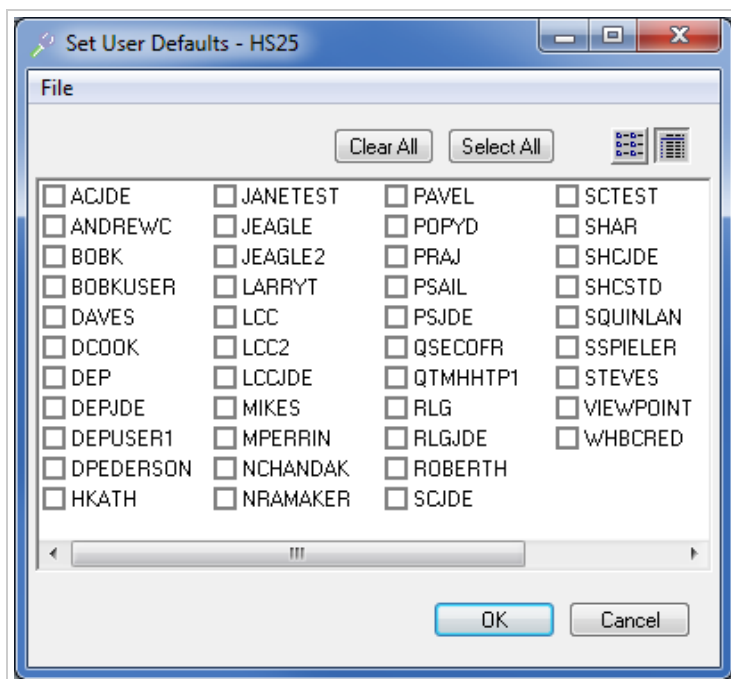
8. Press OK on all remaining screens to finish.

Optional Support for Supplemental Groups

Perform these steps if you need to apply row-level security to supplemental groups.

1. At a command line issue this command to edit the jdedriver.cfg file:
   ```
   EDTF '/rio/lib/jdedriver.cfg'
   ```
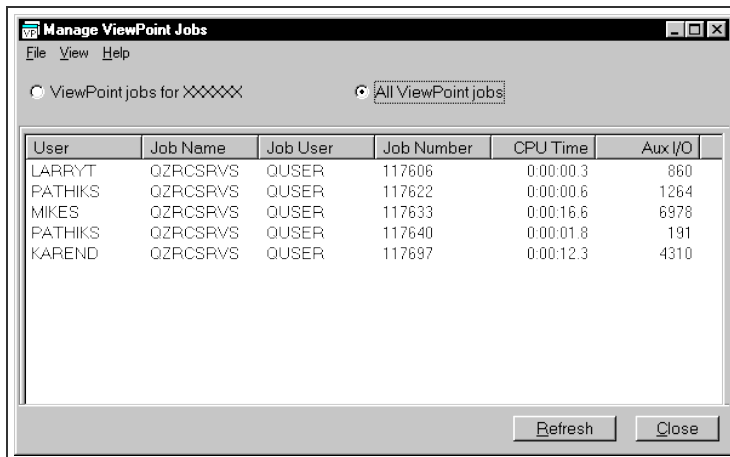
2. In the file editor, use the first blank line available near the top of the file, or insert a new blank line, and add the following statement:
   ```
   JDEDriver.supplementalGroupSupport=TRUE
   ```

3. Press F3 to save and exit the file editor.

Manage Viewpoint Jobs

Use this option to see the status of currently active Viewpoint jobs. Jobs can be cancelled and job logs can be reviewed. Administrators can manage all jobs and users can manage their own jobs.

Options

User - The user name identifies the user id logged onto the Viewpoint session for this job.

Job Name - The name of the job as identified to the system.

Job User - The job user identifies the user who submits the job and the user profile under which the job is run.

Job Number - The system-assigned job number.

CPU Time - The total processing unit time used by the job, expressed in seconds.

AUX I/O - The elapsed number of auxiliary storage I/O operations. This is the number of storage read and write operations the initial thread has made during the measurement time interval. This includes both database and non-database paging.

'Viewpoint jobs for xxxx' - Select to see a list for your jobs only.

'All Viewpoint Jobs' - Administrators will have access to this option in order to see a list of all Viewpoint jobs.

Refresh Button - Press Refresh to regenerate the list of jobs.

Close Button - Press the Close button to exit the Viewpoint Jobs screen.

Menu Options

File \ Close - Close the Viewpoint Jobs dialog and return to the main Administration Control screen.

File \ Delete / End Job - End the selected job(s). You will be presented with an End Job confirmation screen.

File \ Job Log - Display the job log for the selected Viewpoint user.

File \ Exit - Exit completely from the job display and close Administrator.

View \ Refresh F5 - Refresh the list of jobs.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Viewpoint Joblog

This display shows the job messages for a given Viewpoint Job. Messages are color coded based on the type of message. Menu options are available to print, copy and control the list.
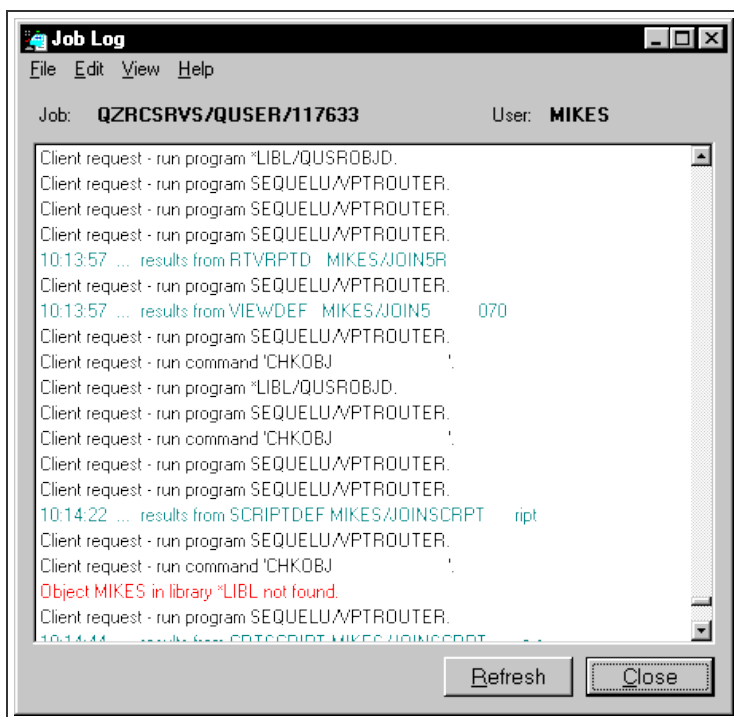
Options

Job - Display of the job/job user/job number.

User - Display of the Viewpoint user associated with the job.

Job Message Display - List of messages for the job. Messages are color coded by message type. Messages can be expanded and sorted using the menu options.

Refresh Button - Press Refresh to regenerate the job messages.

Close Button - Press the Close button to exit the Viewpoint Jobs screen.

Menu Options

File \ Close - Close the Viewpoint Job Log dialog and return to the main Administration Control screen.

File \ Print Setup - Standard print setup dialog to change printer and page orientation.

File \ Print - Print the joblog to a local printer.

File \ Exit - Exit completely from the job log display and close Administrator.

Edit \ Copy all to Clipboard - Paste the job log contents to the windows clipboard.

View \ Ascend - Sort the messages from oldest to newest.

View \ Descend - Sort the messages from newest to oldest.

View \ Expand - Expand the messages to display second level text.

View \ Collapse - Close the second level messages.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Job Log Color Legend

Black	General / informational messages
Blue	Second level messages
Green	Completion messages
Magenta	Notification or diagnostic messages
Teal	Request messages
Red	Escape / error messages

End a Viewpoint Job

When the 'End Job' option is chosen from the Manage Viewpoint Jobs display, an End Confirmation display is presented.

Choose whether to **Cancel** the end job request or **End the Job** (with or without creating a job log).

ViewPoint Job End Confirmation

You have chosen to end the job QZRCSRVS/QUSER/117633. You may end the job immediately with a job log or without.

[End without Job Log]   [End with Job Log]   [Cancel]
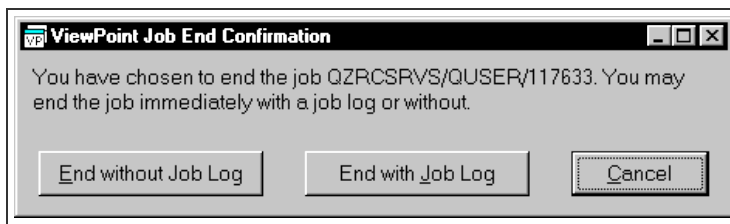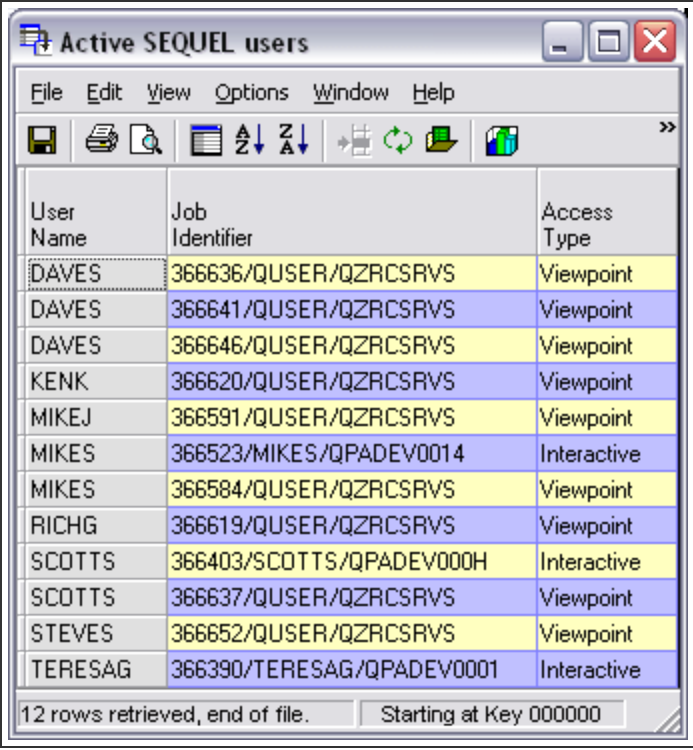
Active Users

Locate Current Jobs

This option displays a list of active Sequel users and the status of their jobs. This is handy before an install of Sequel on the IBM i as Sequel or Viewpoint cannot be in use during an install.

A series or views and scripts are run to locate any and all Sequel/Viewpoint related jobs on the system. Use this display to locate and end jobs if necessary.

Query Options

Administrators can use this feature to maintain user copies of the QAQQINI Query Option File. The Query Option File is used to control how queries are processed for a given user.

You can specify that a Query Option file be used by changing the Sequel Defaults for the user.

The default file in QUSRSYS can be specified or a copy that exists in any library.

The options for a chosen file are displayed in the main part of the screen. Options can be edited, added, or deleted using the menu options.
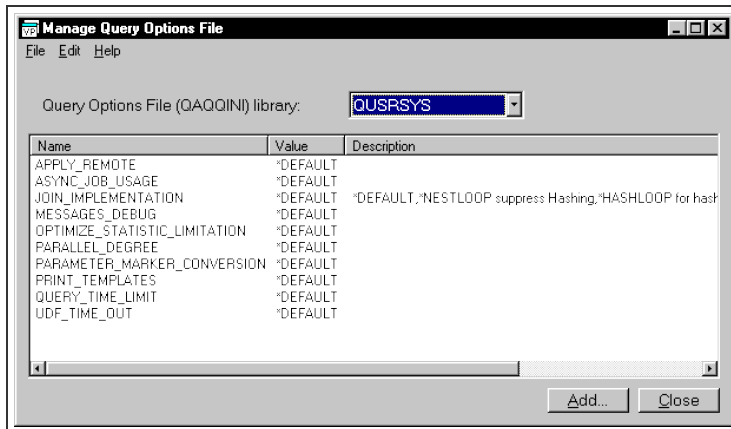
Options

Query Option File Library - Use the drop down list to choose the library that contains the Query Option File.

Name - Name of one of the various options for this file. The different items available and the values are explained in detail at the IBM Info Center.

Value - *DEFAULT or the value selected for this option.

Description - This is supplied when a value other than *DEFAULT is specified.

Add Button - Add an entry to the file.

Close Button - Press the Close button to exit the Option File screen.

Menu Options

File \ Close - Close the Options File dialog and return to the main Administration Control screen.

File \ Exit - Close the Options File dialog and exit the Administration Control screen.

Edit \ Add - Add an entry to the file.

Edit \ Edit - Edit an existing entry.
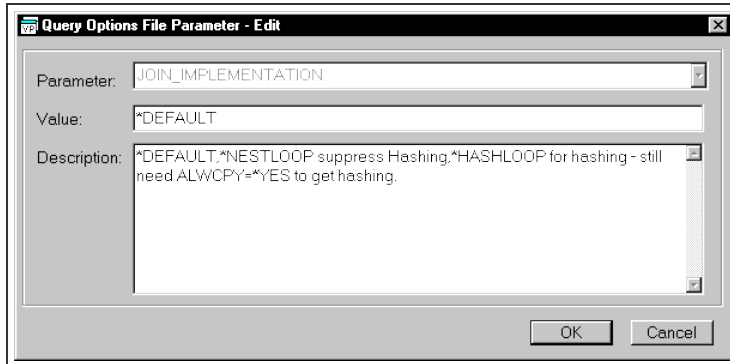
Edit \ Delete - Delete an entry from the file.

Help \ Contents - Open the on line help.

Help \ About - Display Administrator version information.

Query Option Detail

This screen is used to Edit (below), Add, or Delete an Option in the selected Query Option File.

The different parameters and their available values are explained at IBM Info Center.
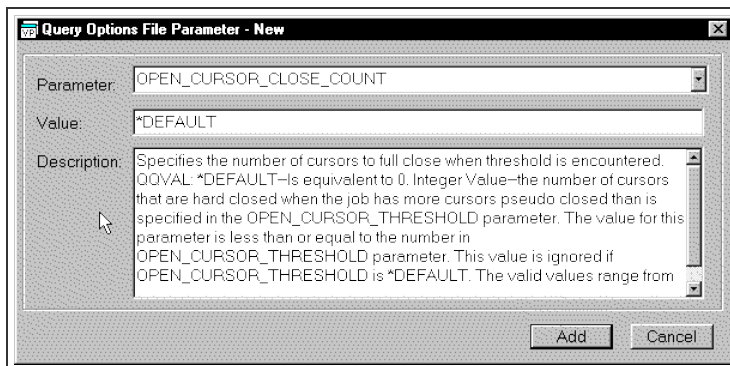
Add

When the add option is chosen, a blank screen is displayed. Choose a parameter from the drop down display. Press the **Add** button to create a ne
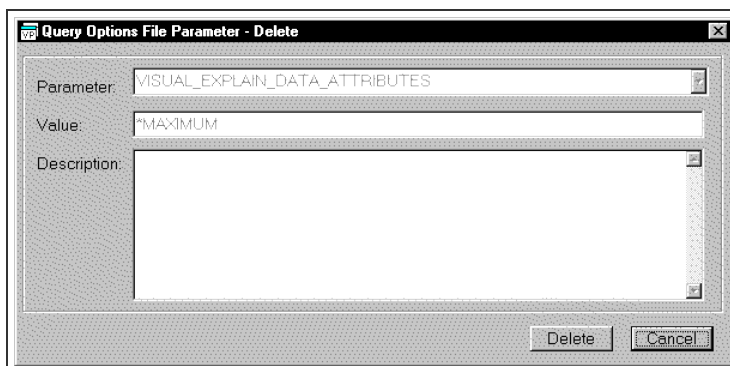
Delete

When the delete option is chosen for an entry, this screen is presented. The parameter, value, and description are filled in. Press the **Delete** button to remove this entry from the option file.

Options

Parameter - Name of the query option parameter.

Value - *DEFAULT or any other allowed value for the parameter.

Description - Description of the parameter and its values.

OK Button - On the edit screen, press to apply any changes.

Add Button - On the new screen, press to add an entry to the file.

Delete Button - On the delete screen, press to remove from the file.

Close Button - Press the Close button to exit the Option File screen.

Help Button - Press Help to access the on line help.

Maintain Host Servers

The Sequel Host file describes connection information that allows Sequel / Viewpoint to connect to remote databases. The Sequel Host List screen below allows for the management of the host file.

Sequel supports connections to DRDA databases defined to the iSeries host (WRKRDBDIRE) and also through Type-4 JDBC drivers.

Definitions will be entered for Platform servers (start with *) and Database servers.

Platform Servers

These servers allow for the definition of 'connection level' parameters. This allows you to define these items once and not duplicate them in the Database server definition.

Five platform servers (start with *) are shipped with Administrator.
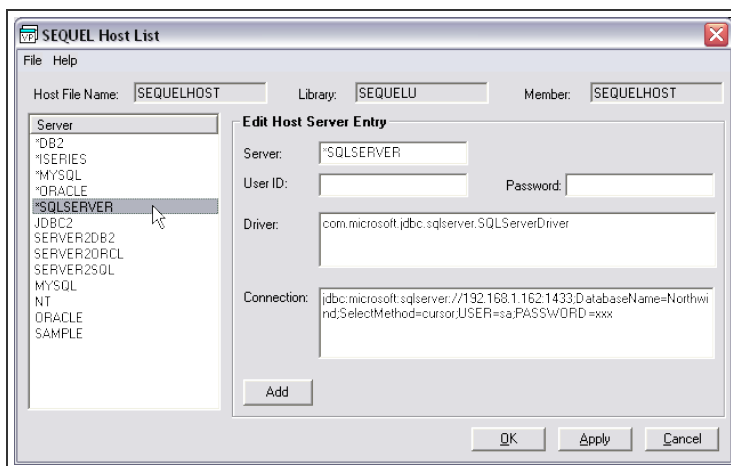
Database Servers

These definitions are specific to the database and/or host you wish to access for a given platform. Information related to the server type, database name, location on the network, user id and password is defined here. This information will be used in conjunction with, or may override settings in the referenced Platform server.
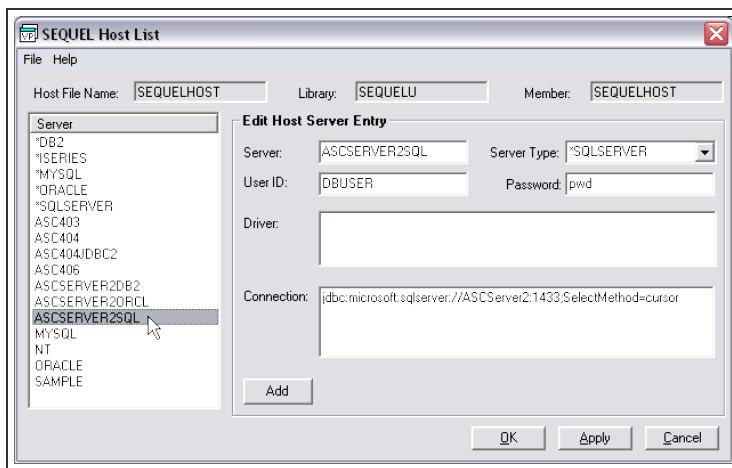
Options

Host File Name, Library, Member - Informational display for the current Sequel Host file. Use **File=>New** to create a different file or member. Use **File=>Open** to work with a different host file.

Server List Window - List of previously defined Platform and Database servers.

Server - Enter the name for a new server definition.

Server Type - This item is only available when creating a new or editing an existing Database server. Select one of the Platform servers from the drop down list.

User ID - Specify the remote user ID under which the request will execute.

> If specified for a Database server, this value will override the value defined in the referenced Platform Server.

Password - Specify the password for the user ID above.

> If specified for a Database server, this value will override the value defined in the referenced Platform Server.

Driver - Name of a Type-4 JDBC driver to access data for this platform. If left blank, then the platform is assumed to be a DRDA platform and must be defined in the iSeries remote database directory (WRKRDBDIRE).

> If specified for a Database server, this value will override the value defined in the referenced Platform Server.

Connection - Information passed to the 'connector' when attempting to link to a given server. This string is connector specific and may include reference to driver type, platform server, location on the network, database name, etc.

> If specified for a Database server, this value will override the value defined in the referenced Platform Server.

Add - Press to place new server definitions into the Server list.

OK - Close window and save changes.

Apply - Apply Changes but leave the list open.

Cancel - Cancel any changes and close window.

SQL Join Database

Manage the SQL Join File

Viewpoint includes an AutoJoin facility to automate the process of joining files. AutoJoin is a user selectable option that draws on information stored in the SQLJOINDB file in the Sequel library.

Use this option to maintain the SQLJOINDB file and create join options for use by Viewpoint's Autojoin feature.
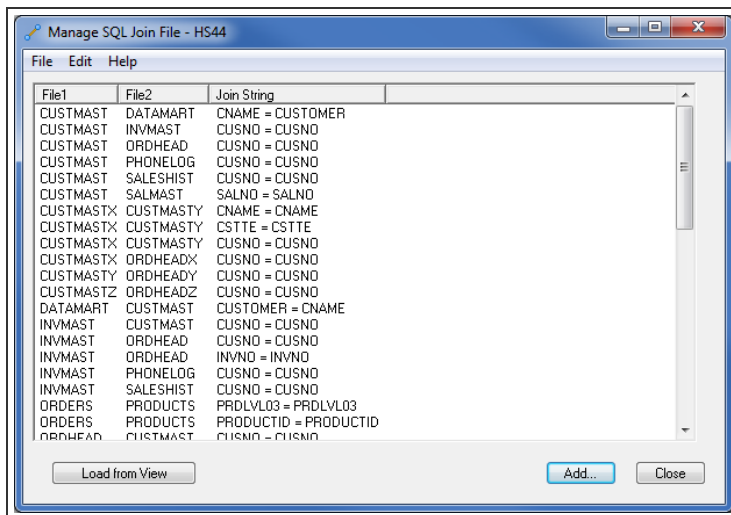
Join statements can be Added directly to the file (Add button) or scanned from existing view (Load from View button).

Add a Join Statement

With this panel you enter a Join statement directly to the SQLJOINDB file. Specify file one and two, and the corresponding fields from each file to use in the Join.
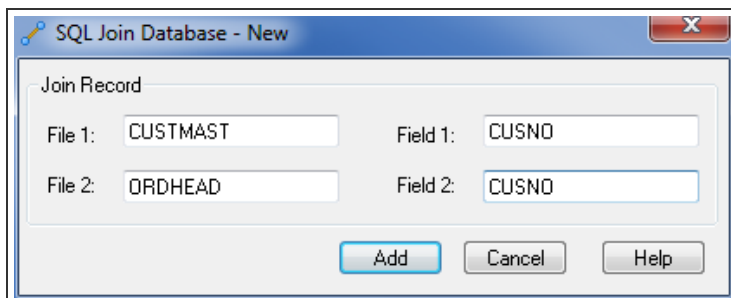
Press the **Add** button to process the request.

Load a Join Statement from a View

Use this option to select views to be scanned for their join statement. The files and join statements are added to the SQLJOINDB file.

Specific views, names with wildcards(*), or all views for a selected (or all) library can be selected.
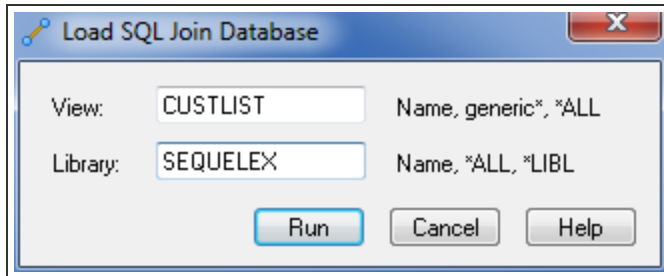
Press the **Run** button to process the request.

Drill Down Options

The option file contains instructions that allow users to run views, programs, etc. from open view results. These options are used in Drill Down Applications. Use this option to view and change the instructions in the selected option file.

When chosen this option will present the Select Option File window below. Navigate to a library and select a file and member.
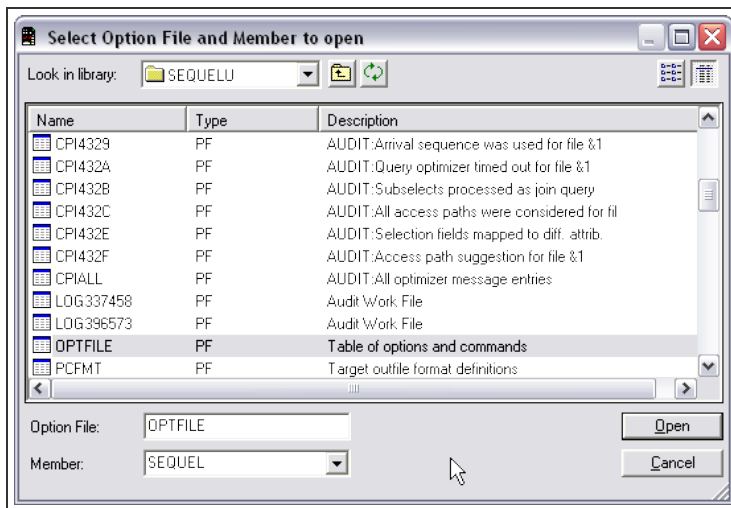
Press **Open** to select the file.
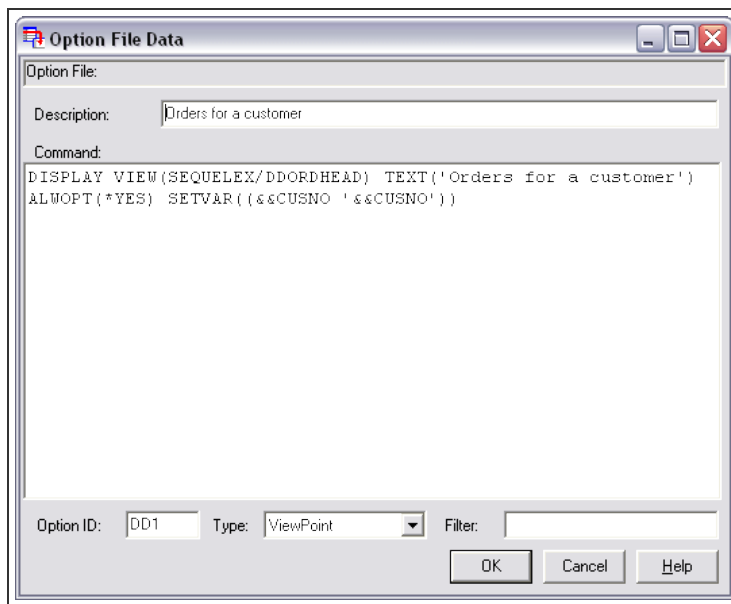
The Drill Down Options screen below lists all Drill Down Application options defined in a given option file.

Review the parameters on this display or right-click an option and select **Edit Option** to open in the edit screen (below).
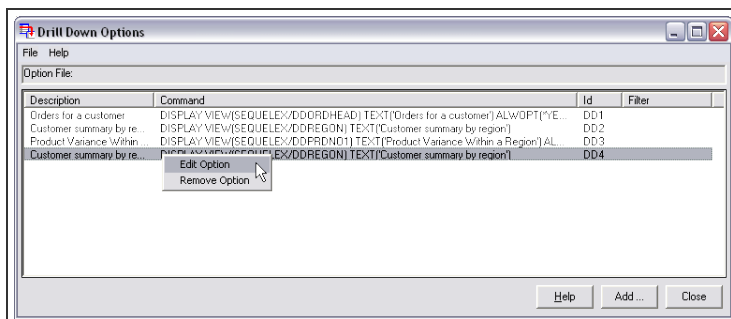
Use the **Add** button to create a new option. A blank Option File Data screen similar to the one below is use to enter parameters for a new option.

The Option File Data display is used to create new options, or maintain existing options.

Dynamic Drill Down List

The Dynamic Drill Down field list displays from Viewpoint by selecting the Regroup / Show Detail option in a grouping view's result window, or when using Drill to Links in a Sequel Drill Down Application. Administrator is used to maintain the file on the IBM i host containing a list of available link fields.

The two main sections in the display below show a list of File Fields to choose from (left) and selected Dynamic Drill Fields (right).
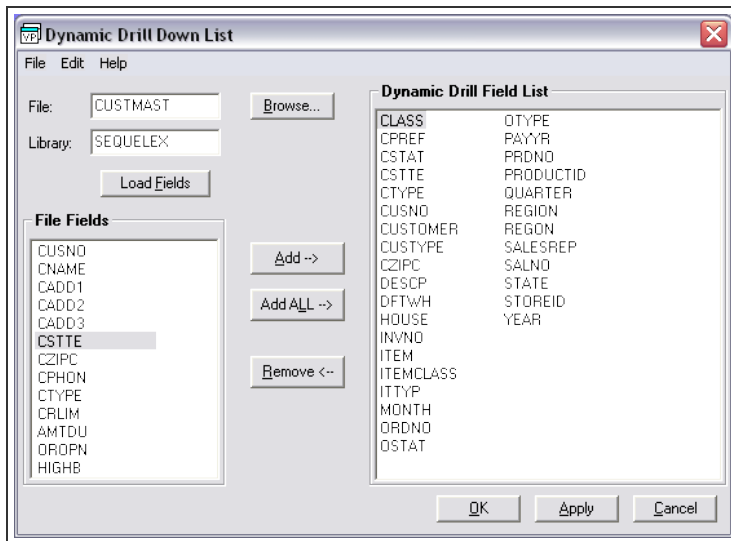
Options

File and Library - Enter the library and name of a file to populate the File Fields list.(below)

Browse Button - Press to open the Select Files screen. Use the folder tree to navigate to a desired file.
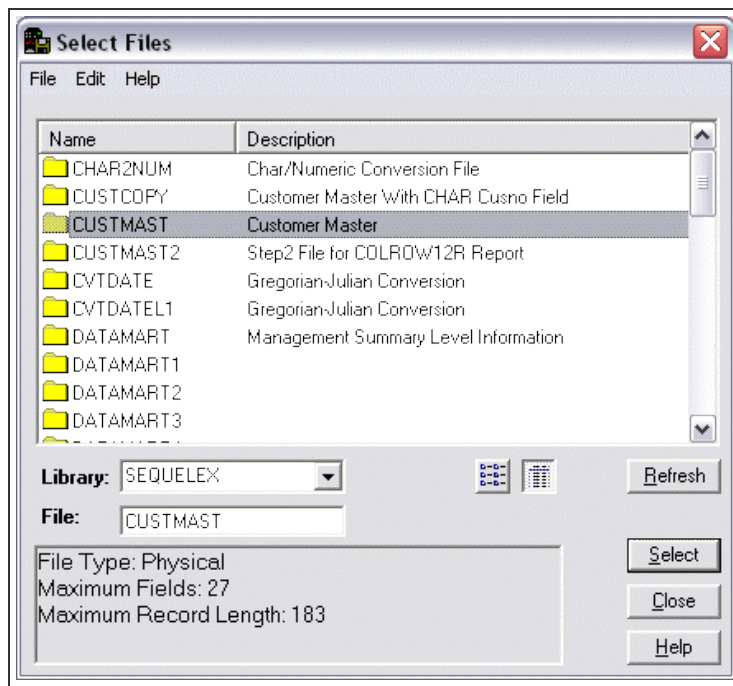
Highlight a file, and press the **Select** button.

Load Fields - Press to populate the File Fields List using the selected file.

File Fields - List of fields from the selected file. Select individually, use Shift-click to select multiple contiguous fields, or Ctl-click to select multiple non-contiguous fields.

Add Button - Press to add selected fields to the Dynamic Drill Field List.

Add ALL Button - Press to add all fields from the selected file to the Dynamic Drill Fields List.

Remove Button - Remove selected fields from the Dynamic Drill Fields List.

Dynamic Drill Field List - List of fields that will be available Dynamic Regrouping view and Drill Down Applications.

OK - Close window and save changes.

Apply - Apply Changes but leave the list open.

Cancel - Cancel any changes and close window.

SWI Function Authorization

Sequel Web Interface (SWI) provides users with browser access to Viewpoint queries, reports, and other objects as well as the ability to create output with these objects and schedule jobs using HelpSystems' Automate Schedule (if configured).

This Administrator feature is used to limit access on a user-by-user basis to many of these functions provided by SWI when connected through a configured Sequel Web Server (SWS in Host mode, not Repository mode).

When selected the Function Authorization screen presents a list of SWI functions that can be restricted. The two tabs present the process in two different views: By function, or by user.

Select by Function

The Select by Function tab shows functions and the users that are restricted from them. You may see any of the following:

- Any function that has locks or exceptions applied to it appear blue and bold in the left panel of the display.
- Users that are locked from a selected function appear red and bold in the right panel of the display.
- Users that are tagged as an exception to a *LOCKALL condition appear green and bold.

Select any function to see the users that are restricted from the function.
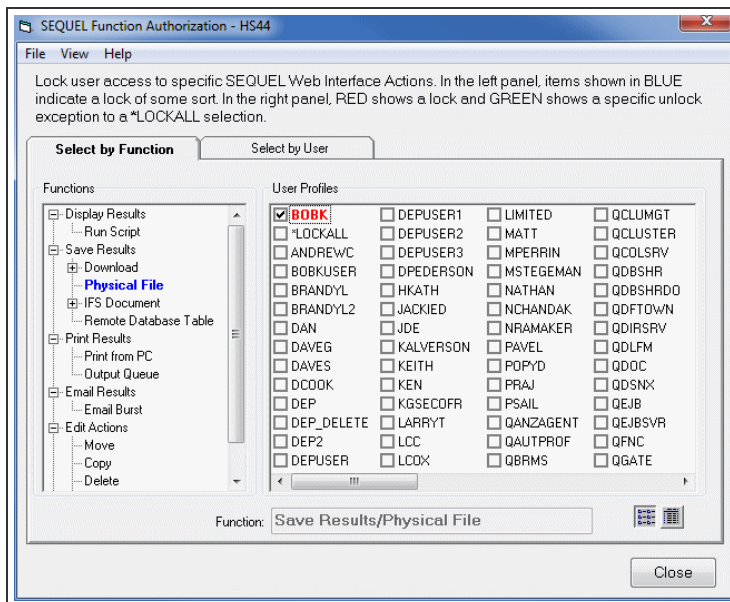
Lock by Function

1. Open the Select by Function tab.
2. Select a function from the list of available functions in the left panel. If you select a main node, like Print Results, all print features will be locked for the selected user.
3. Check individual users to restrict them from the selected function or node.

   They will move to the beginning of the list and their font will change to red and bold.
    or
   Check the special value *LOCKALL to restrict all users from the selected function.

   With *LOCKALL selected, check individual users to add them as an exception to the *LOCKALL condition. *LOCKALL will appear red and bold, and selected users (exceptions) will appear green and bold.
4. To remove a lock, or an exception to a *LOCKALL condition, select the function to see which users are selected and uncheck the user.

Select by User

The Select by User tab shows users and the functions they are restricted from.You may see any of the following:

- Any user that has locks or exceptions applied appear blue and bold in the left panel of the display.
- Functions that are locked from a selected user appear red and bold in the right panel of the display.
- Functions that are tagged as an exception to a *LOCKALL condition appear green and bold.

Select any user to see the functions from which they are restricted.
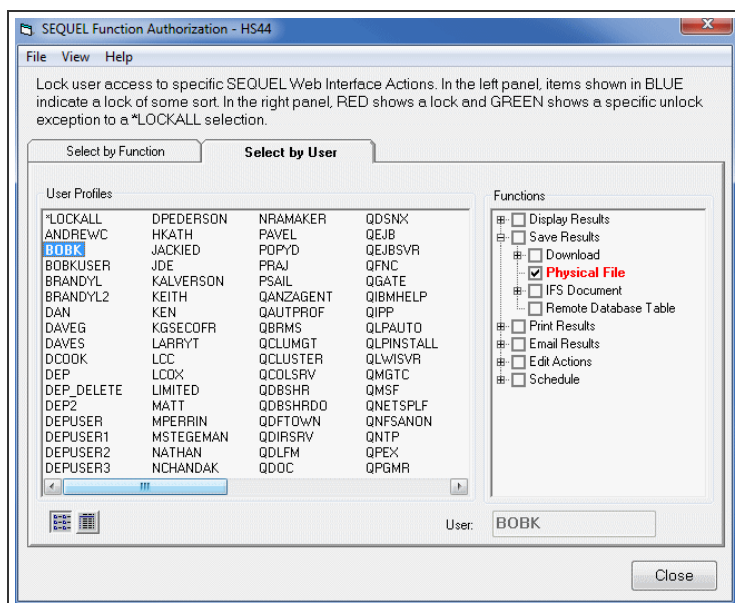
Lock by User

1. Open the Select by User tab.
2. Check individual users from the list of available users in the left panel to restrict them from the selected function.
   or
   Check the special value *LOCKALL to restrict all users from the selected function.

   You can also check individual users to add them as an exception to the *LOCKALL condition. *LOCKALL will appear red and bold, and selected users (exceptions) will appear green and bold.
3. Select a function from the list of available functions in the right panel.
4. To remove a lock, or an exception to a *LOCKALL condition, select the user to see which functions are locked and uncheck the function.

Index