INFINIUM SOFTWARE

Platform Products

Query Security Guide

Notice

The information in this document is subject to change without notice.

Infinium Software, Inc., shall not be liable for any technical or editorial errors contained herein or for incidental or consequential damages resulting from the performance, furnishing, or use of this material.

Printing History

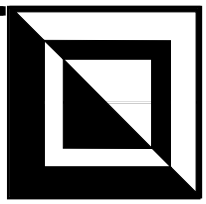
First Edition: September 1993

Latest Edition: August 1999 (Infinium QY Release 2.0)

Document Number: PQY9507141715-03

Table of Contents

About This Guide



This section answers the following questions:

- Who should read this guide?
- What is the purpose of this guide?
- How is this guide organized?
- What conventions are used in this guide?
- Where can you find related information?

Who Should Read This Guide?

This guide is for the people in your organization who are responsible for maintaining user authorization and application security data to be used during Infinium Query report creation and generation.

What Is the Purpose of This Guide?

The purpose of this guide is to describe how to use the options within the Infinium Query *Security Functions* menu.

How Is This Guide Organized?

This guide contains the following parts:

- Introduction to the Security Functions
- Performing Security Conversions
- Using the Security Utilities

- Working with Security Definitions
- Working with Security Authorizations

Part	Title	Description
1	Introduction to the Security Functions	Provides a conceptual background for using the Infinium Query *Security Functions* menu options.
2	Performing Security Conversions	Provides background and step-by-step procedural instructions for generating a security conversion in Infinium Query.
3	Using the Security Utilities	Provides information and instructions for generating the four Infinium Query security reports, and instructions for releasing function locks.
4	Working with Security Definitions	Provides background and instructions for creating, copying, changing, displaying, and deleting Infinium Query library, file, and field security definitions, and for overriding forced file joins.
5	Working with Security Authorizations	Provides background and instructions for customizing an individual user's authority to access specified libraries, files, and fields through Infinium Query.

Note: Since security definitions are overridden at the next security conversion, Infinium recommends that you maintain user authority data through the *Authorizations* functions, not the *Definition* functions.

What Conventions Are Used in This Guide?

The following conventions are used in this guide:

Convention	Description	Example
F3	Keys found on your keyboard are represented by a key symbol.	Press F3 to exit the function.
Menu Options and *Field Names*	Menu options and field names found within the system are represented by *italics*. This document uses the same upper and lower case patterns as the system displays on your terminal.	Select *Security Functions*. Type a valid database library name in the *Library name* field.
Data you type and **System-generated Messages**	Characters, numbers, words, and phrases that you type or messages the system displays are represented by a **bold monospaced** typeface.	Type **GLDBFA** in the *Library name* field. The system displays the following message: **Invalid entry**
Select...	This document instructs you when to select an option from a menu. To select a menu option, position your cursor next to the desired option, type any non-blank character, and then press Enter.	From the *Security Functions* menu, select *Conversions.*

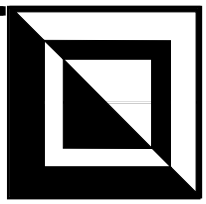
Where Can You Find Related Information?

For more information about Infinium Query, refer to the following documents:

- *Guide to Infinium Query*
- *Infinium Query Administrator's Guide*
- *Infinium Query Release 2.0 Notes*
- *Infinium Query Installing Release 2.0*

Notes

Part 1



Introduction to the Security Functions

This part of the guide provides conceptual background for using the Infinium Query security functions by providing answers to the following questions.

What Is Infinium Query?

Infinium Query is the Infinium application that lets your users generate customized reports containing data gathered from the many Infinium database applications. Infinium Query allows the users to define and generate reports that meet your company's unique needs.

To ensure that users access only database application data with which they are authorized to work, Infinium Query requires conversion of security information for an application prior to the running of reports for that application. Part 2 of this guide provides background information and instructions for performing these security conversions.

What Are Infinium Query Security Conversions?

An Infinium Query security conversion is the process of retrieving applicable user authorization, library, file, field, and value list data from an Infinium application database and recording it in Infinium Query records. The converted data lets the user generate reports based on the database application's records but prevents the user from accessing data for which that user is not authorized.

Infinium Query provides two types of security conversion at the *Conversion* menu. These two types are described in the following table.

Type of Conversion	Use
Infinium Security Conversion This is also known as Application Conversion	Used to convert user, library, file, field, and data restriction information from certain Infinium applications. The security that results from this type of conversion is based on authority levels and data value restrictions in the application. Refer to Part 2 of this guide for more information about these applications, authority levels, and data value restrictions.
Generic Conversion	Used to convert user, library, file, and field information from certain Infinium applications and (if you are using Infinium Query/X) all non-Infinium applications. The security that results from this type of conversion is based only on authority levels. Refer to Part 2 of this guide for more information about these applications and authority levels.

Note: Part 2 of this guide provides a table identifying which Infinium database applications require which type of conversion.

What Terminology Applies to Infinium Query Security?

The following terms are useful for understanding Infinium Query security.

Term	Definition
Security Definition	Information about a user, library file, field, value list, or value structure. Infinium Query uses these definitions to identify libraries, files, and fields available to a user. Infinium Query creates the definitions during conversion.
User definition	A user ID from the user's Infinium Application Manager profile, a user description, and the user's authority level.
Library definition	A library name, a description of the library, and the authority level assigned to that library. Infinium Query uses the authority level with Infinium Query user definition authority levels to identify which libraries are available to that Infinium Query user.
File definition	A file name, description, and authority level. Infinium Query uses the authority level with user definition authority levels to identify files available to a user. In some cases, a file definition also specifies a related file to be used with the current file and the fields that join the two files.
Field definition	A field name, description, and authority level. Infinium Query uses the authority level with user definition authority levels to identify fields available to a user.
Value list definition	Values that records must contain within certain specified fields in order for the user to be allowed to access those records.
Value structure definition	User-specific security restrictions converted to Infinium Query from Infinium application security files.
Authorization	Security information allowing access to specified libraries, files, and fields.

These concepts are further explained in the appropriate sections later in this guide.

What Are the Infinium Query Security Functions?

The Infinium Query *Security Functions* menu provides the following groups of options:

- *Conversion*

  For converting security data from database applications

- *Utilities*

  For generating security reports and releasing locked functions

- *Definitions*

  For displaying and maintaining security information about users, libraries, files, and fields

- *Authorizations*

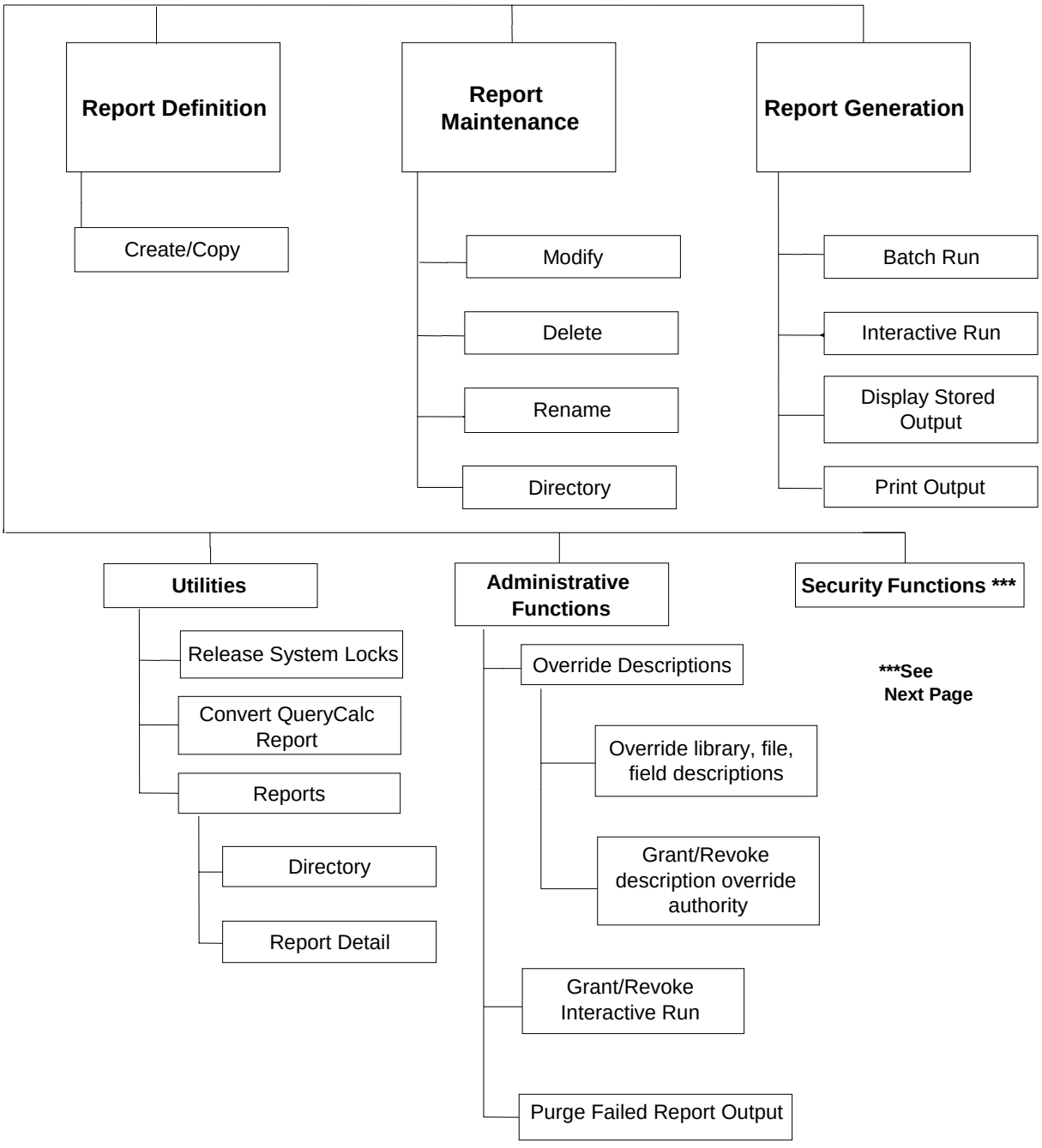
  For displaying and maintaining information about user access to specified libraries, files, and fields

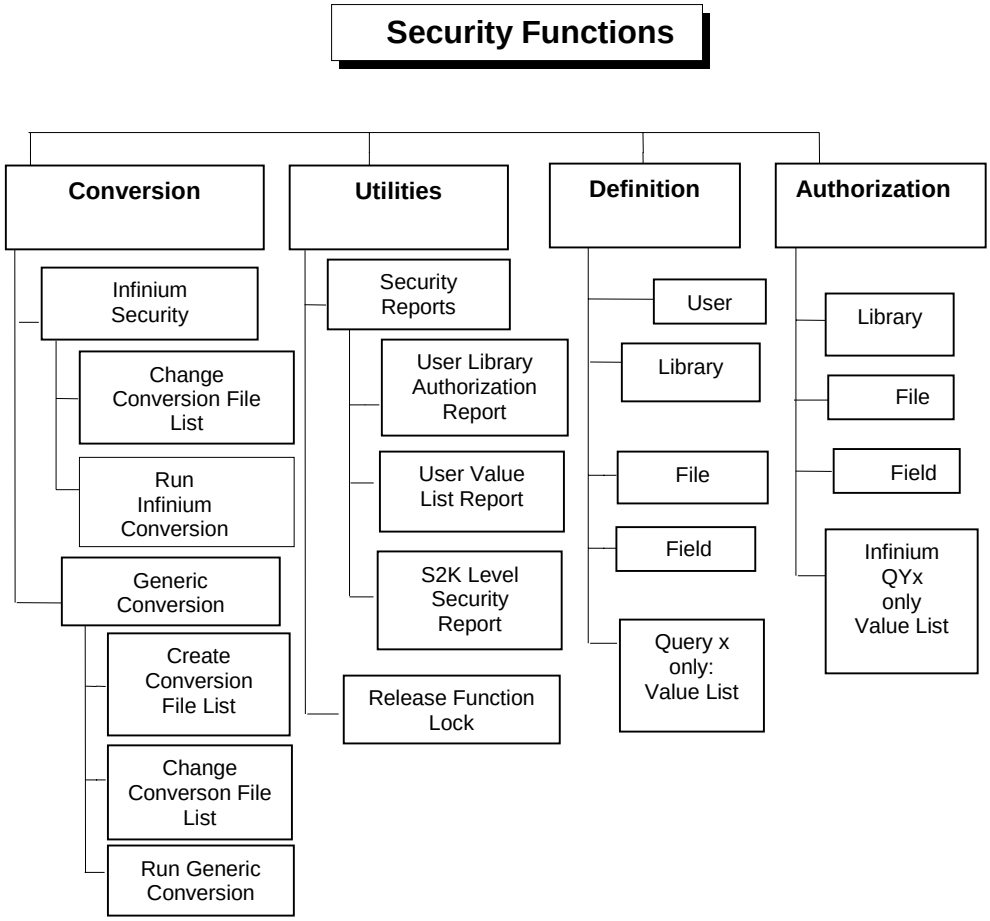
The diagrams on the following pages summarize the following menu structures:

- Infinium Query functions other than the security functions
- Infinium Query security functions

The remaining parts of this guide provide background and instructions for using the conversion, utility, definitions, and authorization functions.

Infinium Query Main Menu




Security Functions
Conversion
Utilities
Definition
Authorization
Infinium Security
Change Conversion File List
Run Infinium Conversion
Generic Conversion
Create Conversion File List
Change Converson File List
Run Generic Conversion
Security Reports
User Library Authorization Report
User Value List Report
S2K Level Security Report
Release Function Lock
User
Library
File
Field
Query x only: Value List
Library
File
Field
Infinium QYx only Value List

Who Can Use the Infinium Query Security Functions?

Authorization Restrictions

Because of the sensitive nature of data security, access to the *Security Functions* menu is limited as follows:

- You must sign on as **QY2000**, the standard Infinium Query supervisor user, if you want access to all the *Security Functions* menu options.
- You must have an authority level of **1** in your Infinium Query user definition record to use the *Security Functions* menu's *Conversion* options, if you sign on as any user other than **QY2000**. You cannot access any other *Security Functions* menu options in this case.

Infinium Query User-Definition Authorization

An Infinium Query user definition record can have a different authority level than the corresponding Infinium Application Manager user profile for that user. The authority level in the Infinium Query user definition record is valid only within Infinium Query.

The Infinium Query security conversion process puts the user's Infinium Application Manager user profile authorization level into the Infinium Query user definition record. After conversion, a user signing on as **QY2000** can change the authority level in the Infinium Query user definition.

Note: If you make this change by using the *Definitions* functions, the change lasts only until the next conversion process. Infinium therefore recommends that you use the *Authorizations* functions rather than the *Definitions* functions to modify a user's authorization.

Part 2

Performing Security Conversions

This part of the guide provides background and instructions for performing conversions of security information. When you use an Infinium Query security conversion function for a designated database application, the system converts security information from the application's records and Infinium Application Manager records to Infinium Query security records.

WARNING

To convert security for database applications from any other vendor than Infinium, you must purchase, install, and use Infinium's product Infinium Query/Extended (Infinium Query/X). If you try to convert security for any database other than an Infinium database using Infinium Query rather than Infinium Query/X, the system displays an error message and stops the conversion process.

This part of the guide covers the following topics.

Understanding Infinium Query Security Conversion

This section provides details about the layers of security and the security rules that apply to the generation of reports through Infinium Query or Infinium Query/Extended. To generate an Infinium Query report, a user must be authorized to access all three of the following:

- The Infinium Query system
- The Infinium Query report definition used to generate the output
- The database libraries, files, records, and fields the report uses

The following subtopics provide details about these and related requirements as well as other background information:

- Role of User's Profile in Infinium Application Manager
- Baseline Application Database File Protection
- Security Levels Assigned to Users and Database Objects
- Customizing Security for Infinium Query Access to Files
- Security Levels Assigned to Infinium Query Report Definitions
- Checklist for Security Conversions
- Two Types of Infinium Query Security Conversion
- What Happens During a Security Conversion

Role of the User's Profile in Infinium Application Manager

Infinium Application Manager provides the first level of Infinium Query security. No user can access Infinium Query without being authorized to do so in the user's Infinium Application Manager user profile.

Once the user is granted access to Infinium Query, the following applies:

1. When the user presses F2 to access the Action Bar, types **S** for systems, and presses Enter to display a list of the systems the user is authorized to work in, the system selection window includes Infinium Query as a valid choice.
2. When the user accesses Infinium Query to define and run reports, the user is allowed to work only with those database application libraries, files, and fields that meet the following requirements:
   - The user is authorized to access the library, file, and field either in the user's user profile and any application-specific value-based security records.
   - The user has an authority level with a number equal to or lower than the authority level associated with the library, file, or field.
   - The security records for the application have been converted to Infinium Query security records.

Caution: The conditions of the first requirement mean that a user with sufficiently broad authority can use Infinium Query to access data in an application database to which that user does not ordinarily have access through Infinium Application Manager.

Exceptions: For exceptions to the preceding information, refer to the Customizing Security for Infinium Query Access to Files suptopic later in this section.

Baseline Application Database File Protection

The data stored in database libraries for your Infinium database applications is protected by the security features associated with those applications and local Infinium Application Manager user profile records.

Infinium Query prevents users from bypassing this security by requiring conversion of each application's security records to Infinium Query records. This provides the same protection of your files for users accessing the files through Infinium Query as for users accessing the files through the database applications themselves.

Security Levels Assigned to Users and Database Objects

User Security Levels

Each user is assigned a security level in the Infinium Application Manager user profile. The level is anywhere from 1 to 9. Level 1 is the highest, allowing the most privileges for accessing information. The conversion process initially sets the user's level for the Infinium Query system to the level currently in that user's Infinium Application Manager profile.

The Infinium Query Security Supervisor can modify the user's level by using the Infinium Query security functions described in Parts 4 and 5 of this guide.

Database Object Security Levels

Each library, file, and field is also assigned a security level, from 1 to 9, in Infinium Query during the security conversion process, as described in the What Happens During a Security Conversion subtopic later in this section.

A user is authorized to access only those libraries, files, and fields that have a security level number equal to or higher than the user's security level. Example: User A with a security (authorization) level number 5 can access libraries, files, and fields with security level numbers 5 through 9.

During Infinium Query report definition, the user selects one or more libraries, then files, and then fields to be used in the report. At each of these selection levels, the system checks the user's authorizations and displays for potential selection only those libraries, files, and fields this user is authorized to access for Infinium Query reporting purposes.

See the following subtopic for exceptions to this baseline security.

Customizing Security for Infinium Query Access to Files

Sometimes it is desirable to have the security applied through Infinium Query differ for a given user, library, file, or field from the security applied for that user, library, file, or field in the database application.

For example, you may want to assign the definition and generation of certain management reports to a user who does not normally have access to the data needed for those reports. Infinium Query allows you to modify the baseline converted security in the Infinium Query records to allow the necessary read-only access to the data, and to make other similar customizations of the Infinium Query security rules for accessing the data.

Refer to Parts 4 and 5 of this guide for details about this customization.

Security Levels Assigned to Infinium Query Report Definitions

Infinium Query also provides report-specific security. Application security controls only whether a given user can access data in the database to generate a report. Report security controls whether a user can access a report definition to perform either or both of the following tasks:

- Modify the report definition
- Run the report definition to generate the report

The user creating or modifying the report definition sets these controls, including a report security level number from 1 to 9. Users with a security level number higher than the report's security level number cannot access the report definition or run the report.

The user creating or modifying the report definition can also restrict modification and generation of the report to a designated report owner. For more infomation, refer to the Setting Report Controls topic within Part 4 of the *Guide to Infinium Query*.

Checklist for Security Conversions

The following checklist provides guidelines and warnings important for understanding and effectively using the Infinium Query security conversion functions.

- When planning to use the Infinium Query *Security Functions* menu's conversion functions, sign on as **`QY2000`**.
- Before performing security conversions, ensure that all users you will authorize to access database applications through Infinium Query are authorized in Infinium Application Manager to access Infinium Query and are authorized to access the relevant database applications.

  The security conversion process includes conversion of data from each user's profile in Infinium Application Manager.

  Note: The users must be authorized to access the specific version of Infinium Query that you are using to run the conversion. For

example, if you are using the system version 000 to run the conversion, ensure that the relevant users are authorized to access Infinium Query version 000. If you are using a version 020 to run the conversion, ensure that the relevant users are authorized to access Infinium Query version 020.

- Before performing security conversions, ensure that all users you will authorize to access database applications that have application-specific security records are already given the appropriate privileges within those application-specific security records.

  The conversion process does not create Infinium Query user definitions for users of these applications unless the users are defined within these application's own security records. In such cases, you must manually define the user through the *User* option on the Infinium Query Security *Definitions* menu as explained in Part 4 of this guide.

- Whenever you change the security configuration of a database application, repeat the conversion of the application's security to Infinium Query security records to update Infinium Query with the changes.

- Remember that overriding converted security information within Infinium Query, as described in Parts 4 and 5 of this guide, affects only access to data through Infinium Query. It does not affect the baseline security for the database applications themselves.

WARNINGS

User profile QY2000 has security level 0. Anyone signed on as **`QY2000`** has access to all data. Be cautious when assigning use of this profile.

To convert non-Infinium database application security, you must use Infinium Query/Extended (Infinium Query/X) rather than the basic Infinium Query product.

Two Types of Infinium Query Security Conversion

The following table summarizes the two types of security that Infinium Query lets you convert, the menu to use for converting each type, the applications using that type of security, and an explanation of each type.

Type of Security	*Conversion* Menu Option	Applications Using This Type	Explanation of Conversion
Application	*Infinium Software Security*	Infinium Occupational Health Infinium Fixed Assets Infinium Human Resources Infinium Payables Ledger	Converts application-specific security information for users, libraries, files, fields, and data-specific access restrictions. Example: Includes restrictions such as limiting User A to records with particular field values within particular files.
Generic	*Generic Conversion*	Infinium Accounts Receivable Infinium Materials Management Infinium General Ledger All other Infinium database applications not listed in the preceding row of this table For only Infinium Query/X: All non-Infinium database applications	Converts security information to define the security levels of users, libraries, files, and fields for access through Infinium Query. Example: Specifies whether an Infinium Query user can access or is prevented from accessing each converted library, file, and field.

Both types use Infinium Application Manager user profile information to identify which users can access which libraries, files, and fields. Application security uses additional application-specific value-based security that limits a user to records containing specified values.

What Happens During a Security Conversion

When you submit a conversion, the system creates the following Infinium Query security records with summary data about each item, including, but not limited to, the information cited in the following table:

Infinium Query Record	If *Infinium Security* Conversion	If *Generic Conversion* Conversion
User Definition For each user authorized to access both Infinium Query and the database application	Includes data from: Infinium Application Manager The database application	Includes data from: Infinium Application Manager
Library Definition For the Database Application	Includes a default security level **5**	Includes the security level you specified when creating the conversion file list
File Definition For Each File Included in the Conversion	Includes the security level you accepted or typed at the Change Conversion File List screen	Includes the security level you accepted or typed at the Change Conversion File List screen
Field Definition For Each Field Included in Each of the Files	Includes the same security level as in the related file's Infinium Query definition	Includes the same security level as in the related file's Infinium Query definition
Value List Definitions Corresponding to the Value List Security Items Defined in the Database Application	Includes: The definition The authorization The attachment	Not created
Value List Structure Definitions Corresponding to the Structures Defined in the Database Application	Includes sets of multiple value-specific tests a user must pass to access the data in specified records	Not created
Value List Data For Each User	Includes user-specified field-value security from the database application	Not created

Refer to Parts 4 and 5 of this guide for procedures to edit these records.

Accessing the *Conversions* Menu

Perform these steps to access the Infinium Query *Conversions* menu:

1. At the Infinium Query main menu, select *Security Functions*.
2. Select *Conversion*. The system displays the *Conversions* menu, illustrated in Figure 2-1.

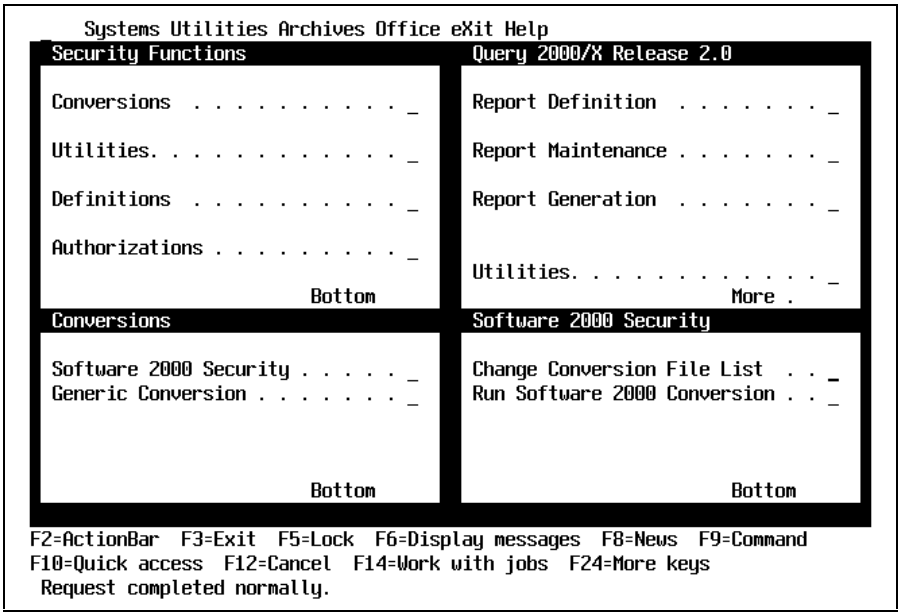


Figure 2-1: Security Conversion Menu (lower left quadrant of screen)

When you select either of the *Conversions* menu options, the system displays the function menu for that type of conversion.

The following topics provide step-by-step procedural instructions for using the two sets of conversion functions.

Using the *Infinium Security* Menu

Applications That Require This Type of Conversion

The *Infinium Security* menu applies to security conversion for the following Infinium database applications:

- Infinium Fixed Assets
- Infinium Occupational Health
- Infinium Human Resources
- Infinium Payables Ledger

Infinium Security Menu Options

The *Infinium Security* menu provides the following two functions, corresponding to the two application security conversion tasks:

- *Change Conversion File List*

  This function lets you specify the file definitions to be converted and modify the file descriptions and security levels for Infinium Query use. This does not change the file descriptions and levels for the application itself.

- *Run Infinium Conversion*

  This function lets you submit the security conversion job.

The following pages provide details about these two functions.

Preparing the Infinium Security Conversion File List

Infinium ships a file list with default security level **5** on each file when shipping a database application that requires using the *Infinium Security* conversion function. Infinium Query lets you maintain the file list for Infinium Query security conversion. The edits do not affect security associated with the direct use of the database application itself.

To review and modify the conversion file list prior to performing the actual conversion for each database application, perform the following steps:

1. At the *Infinium Query Conversions* menu select *Infinium Security*.
2. Select *Change Conversion File List*. The system displays the following screen.

```
 5/23/95    16:45:01     Change Conversion File List      SMGS2KCHG  SMDS2KCH

Type Software 2000 application code, press Enter.


Application . . . . . .  AP
Library Name. . . . . .  APDBFA070_









F3=Exit  F10=Quick access  F12=Cancel
```

Figure 2-2: Infinium Security Change Conversion File List screen

3. Type a valid system designator in the *Application* field. The valid values are AP, EM, FA, HR, and PL.
4. Type the locally-used name of that application's database library in the *Library Name* field. If your site uses the default library names supplied by Infinium, the database library name is the system designator followed by DBFA, such as APDBFA or HRDBFA.
5. Press Enter to display the Conversion File List screen with a list of the files in that library, illustrated in Figure 2-3.

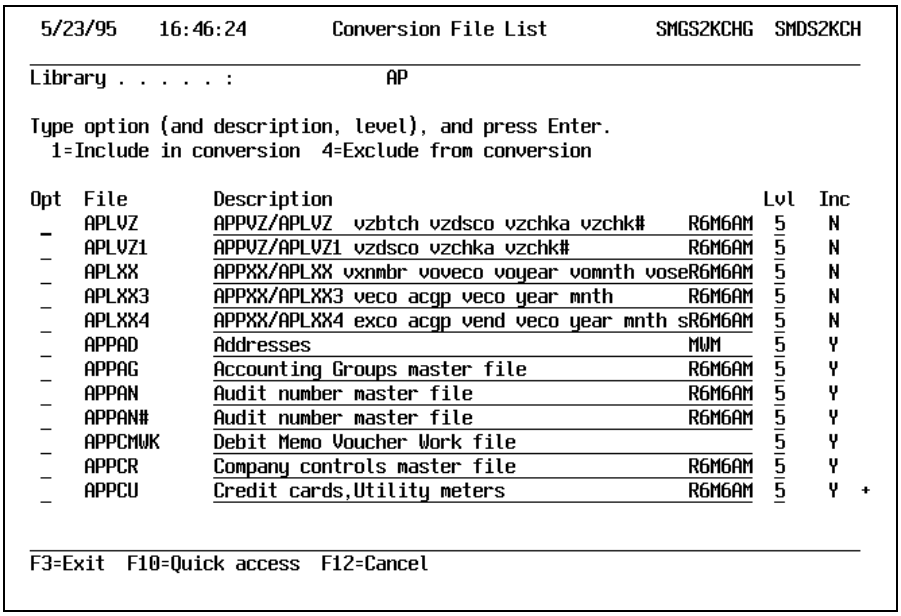


Figure 2-3: Infinium Security Conversion File List screen

6. Press PgDn to go to the physical files, identified by **P** in the third position. The logical files, identified by **L** in the third character position, are listed before the physical files.

   Logical files are listed so that technical personnel can define reports with data from logical files if necessary.

7. Review the list of physical files, descriptions, security levels, and the *Inc* (for Include) values.

   The display-only *Inc* field value indicates whether a file and its description is to be included in (Y) or excluded from (N) the conversion process. The default for physical files is Y, to include them. The default for logical files is N, to exclude them.

8. Use the table on the following page to modify the file list to specify which file descriptions are to be converted.

Goal	Action
To change *Inc* value from **Y** to **N** , to exclude the file and its definition from the conversion process	Type **4** in the *Opt* field next to the file's name.
To change *Inc* value from **N** to **Y**, to include the file and its definition in the conversion process	Type **1** in the *Opt* field next to the file's name.
To modify the file description users will see during report definition	Edit the value in the *Description* field. **Note:** See Part 4 of this guide for modifying the description after conversion.
To change the security level for a file and all its fields	Edit the value in the *Lvl* field. **Note:** See Part 4 of this guide for modifying individual field levels after conversion.

9. Press F3 twice to exit back to the *Infinium Security* menu.

Performing Infinium Security Information Conversion

Once the file list specifies the files to be converted, the descriptions to be displayed to Infinium Query users, and each file's Infinium Query security level, you are ready to perform the conversion.

> **Caution**: Ensure that users are signed off Infinium Query and that no one is modifying the database application's security information during the conversion process.
>
> A conversion could take several hours. You may want to perform the conversion at night or on a weekend to minimize disrupting user schedules and the risk of users signing on.

Perform the following steps to complete the conversion:

1. At the *Infinium Security* menu select *Run Infinium Conversion* to display the Run Infinium Conversion screen.

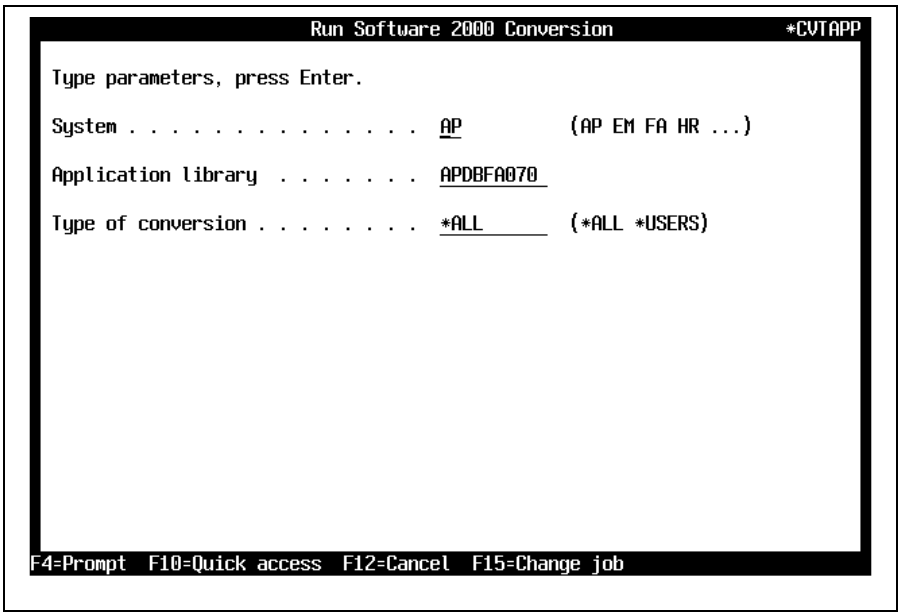


Figure 2-4: Run Infinium Conversion screen

2. Type the two-character system designator for the database application (**AP**, **EM**, **FA**, **HR**, or **PL**) in the *System* field.
3. Type the name of the database library, such as **HRDBFA**, in the *Application library* field.
4. Type ***ALL** or ***USERS** in the *Type of conversion* field.
5. Refer to the explanation on the following page for these values.

The following table explains the uses and effects of the ***ALL** and ***USERS** values:

Value	Effect	When to Use
***ALL**	Converts security information for the library, its files, their fields, value lists, value structures, and for each user who is authorized as follows: In Infinium Application Manager, authorized to access Infinium Query In the application, authorized to access that application	The first time you perform security conversion for this database application Each time you install a new release of this database application When unusual circumstances require refreshing the entire set of Infinium Query security records that control Infinium Query access to the database application
***USERS**	Converts only user security information and only for users who are authorized as follows: In Infinium Application Manager, authorized to access Infinium Query In the application, authorized to access that application	When you need to refresh user-specific Infinium Query security information for your users of the database application due to one of the following: Personnel changes Changes to application security for one or more users

6. Press Enter to submit the conversion as a batch job.

   The system displays informational messages and returns you to the *Infinium Security* menu.

Using the *Generic Conversion* Menu

Applications That Require This Type of Conversion

The *Generic Conversion* menu applies to the following:

- Infinium Accounts Receivable
- Infinium Materials Management
- Infinium General Ledger
- Other Infinium applications not listed elsewhere as requiring the *Infinium Security* function conversion
- All non-Infinium database applications (use Infinium Query/X)

Infinium Query Files That Require This Type of Conversion

Infinium Query lets you generate physical file output for a report or series of reports and then use the output files as sources for other reports. This helps you perform such tasks as building summary reports from a series of previously-run detailed reports.

Infinium Query stores these physical files in library IQY2000. You must convert library IQY2000 if you plan to generate physical files to be used as input to other Infinium Query reports. Refer to the conversion procedure later in this section for details about which files to exclude from the conversion of library IQY2000.

The *Generic Conversion* Menu Options

The *Generic Conversion* menu provides the following three functions, corresponding to the three generic security conversion tasks:

- *Create Conversion File List*

  This function creates a list of the files that are in the target application's database library.

- *Change Conversion File List*

  This function lets you display the file list, specify the files to be converted, and modify their descriptions and security levels for Infinium Query use. This does not change the file descriptions and levels for the application itself.

- *Run Generic Conversion*

  This function lets you perform the actual security conversion.

The following pages provide details about these three functions.

Creating the Generic Conversion File List

You must create a file list before performing a generic conversion.

Perform the following steps to create a list of all the available files in the database library for the application whose security you are converting:

1. At the *Security Functions* menu select *Generic Conversion*.
2. Select *Create Conversion File List* to display the following Create Conversion File List screen.

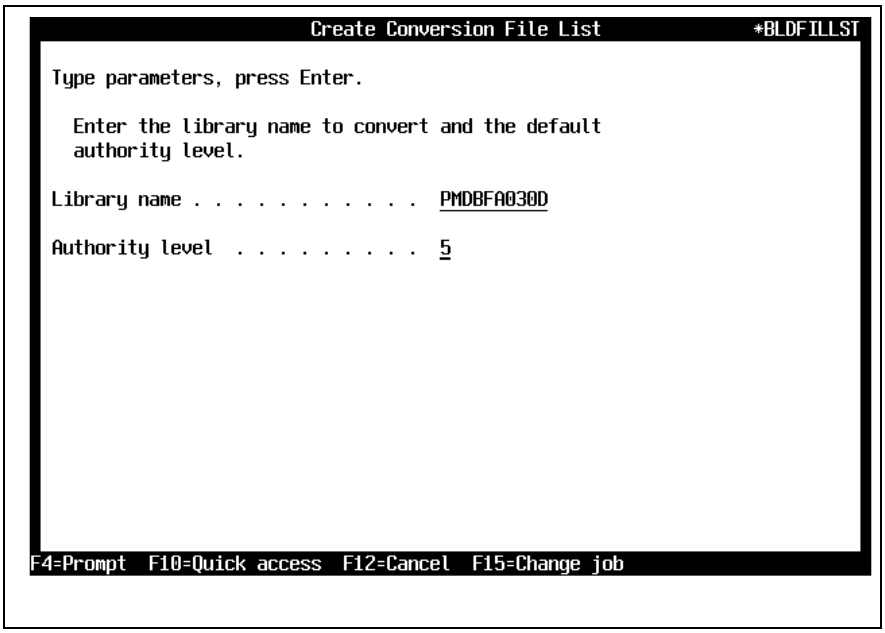


Figure 2-5: Create Conversion File List screen

3. In the *Library name* field, type the name of the library for which you are creating the conversion file list.
4. In the *Authority level* field, type a number from **1** to **9** to indicate the default security level you want assigned to each file in this library for Infinium Query purposes. To indicate the highest security level, type **1** in the *Authority level* field.
5. Press Enter to create the file list for the designated library.

   The system displays informational messages and returns you to the *Generic Conversion* menu.

Reviewing and Modifying the Generic Conversion File List

Infinium Query lets you modify the file list for Infinium Query security conversion purposes. The edits do not affect security associated with the direct use of the database application itself.

Perform the following steps to review and modify the conversion file list prior to performing the actual conversion for each database application.

1. At the *Infinium Query Conversions* menu select *Generic Conversion*.

2. Select *Change Conversion File List*. The system displays the following screen.

```
 5/23/95    17:09:08     Change Conversion File List      SMGGENCHG  SMDGENCH

Type any character to select library(s), press Enter.

Sel  Library     Description
 _   IQY2000     Query 2000 - Release 2.0
 _   PMDBFA030D  Purchase Management 3.0 Development data
 _

F3=Exit  F10=Quick access  F12=Cancel
```

Figure 2-6: Generic Conversion Change Conversion File List screen

3. Type any character in the *Sel* field next to the library that contains the files.
4. Press Enter. The system displays the Conversion File List screen.

```
 5/23/95    17:09:55        Conversion File List          SMGGENCHG  SMDGENCH

Library: PMDBFA030D

Type option (and description, level), and press Enter.
  1=Include in conversion  4=Exclude from conversion

Opt  File        Description                                  Lvl  Inc
 _   PMPPD       Purchase Order Detail                        9    Y
 _   PMPPDW2     Purchase Order Detail work file              9    Y
 _   PMPPG       P.O. Additional Charges                      9    Y
 _   PMPPGWK     PO Additional charges work file              9    Y
 _   PMPPH       Purchase Order Header                        9    Y
 _   PMPPHJ      PO header join to PO detail for OPNQRYF      9    Y
 _   PMPPR       P.O. Receipts                                9    Y
 _   PMPPRJ      OPNQRYF work file to join PO receipts and PO dtl  9  Y
 _   PMPPRWK     P.O. Receipts                                9    Y
 _   PMPPS       P.O. Multi-Ship                              9    Y
 _   PMPPSWK     P.O. Multi-Ship work file                    9    Y
 _   PMPRA       Requisition Multi-Account                    9    Y  +

F3=Exit  F10=Quick access  F12=Cancel
```

Figure 2-7: Generic Conversion Function Conversion File List screen

5. Press PgDn to go to the physical files, identified by **P** in the third position. The logical files, identified by **L** in the third character position, are listed before the physical files.

   Logical files are listed so that technical personnel can define reports with data from logical files if necessary.

6. Review the list of physical files, descriptions, security levels, and the *Inc* values. The display-only *Inc* field value indicates whether a file is to be included in (**Y**) or excluded from (**N**) the conversion process.

   The default for physical files is **Y**, to include them and their descriptions in the conversion process. The default for logical files is **N**, to exclude them and their descriptions from the conversion process.

7. Use the table below to modify the file list as desired.

Goal	Action
To change *Inc* value from **Y** to **N**, to exclude this file definition from the conversion process	Type **4** in the *Opt* field next to the file's name.
To change *Inc* value from **N** to **Y**, to include this file definition in the conversion process	Type **1** in the *Opt* field next to the file's name.
To modify the file description users will see during report definition	Edit the value in the *Description* field. **Note:** See Part 4 of this guide for modifying the description after conversion.
To change the security level for a file and all its fields	Edit the value in the *Lvl* field. **Note:** See Part 4 of this guide for modifying individual field levels after conversion.

Note: If you are converting file descriptions for library IQY2000, exclude all the files that have names beginning with the following strings of letters:

- SMP
- SML
- QYP
- QYL

8. Press F3 twice to exit back to the *Generic Conversion* menu.

Performing the Generic Security Information Conversion

Once the file list specifies the files to be converted, the descriptions to be displayed to Infinium Query users, and each file's Infinium Query security level, you are ready to perform the conversion.

Caution: Ensure that users are signed off Infinium Query and that no one is modifying the database application's security information during the conversion process.

A conversion could take several hours. You may want to perform the conversion at night or on a weekend to minimize disrupting user schedules and the risk of users signing on.

Perform the following steps to complete the conversion:

1. At the *Generic Conversion* menu select *Run Generic Conversion* to display the Run Generic Conversion screen.

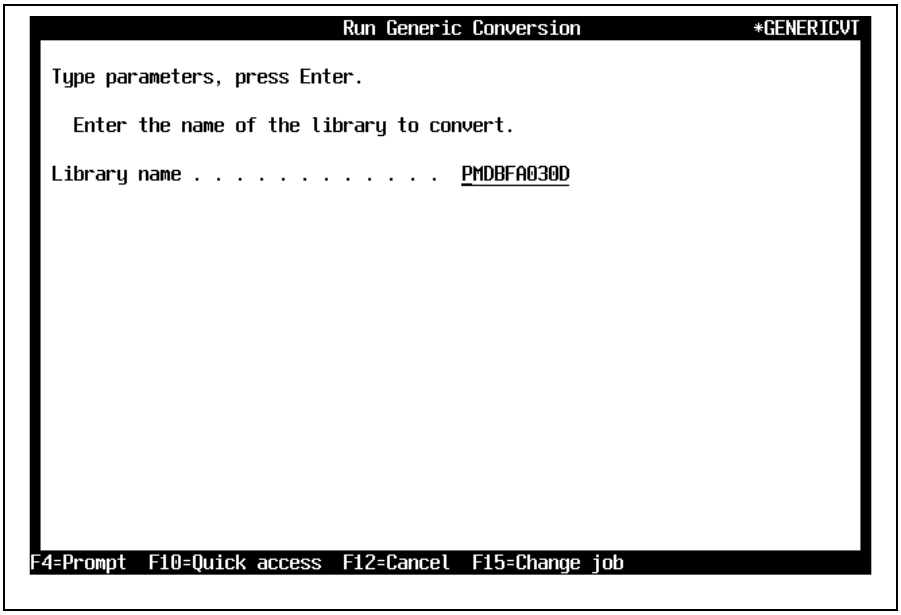


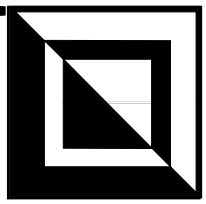
Figure 2-8: Run Generic Conversion screen

2. In the *Library name* field, type the database library name for the application whose security you are converting, such as **HRDBFA**.
3. Press Enter to submit the conversion as a batch job.

   The system submits the job and returns you to the *Generic Conversion* menu.

Notes

Part 3



Using the Security Utilities

This part of the guide explains how to use the following Infinium Query security *Utilities* menu options:

- *Security Reports*
- *Release Function Lock*

The following table summarizes the tasks covered.

Accessing the Security *Utilities* Menu

Perform the following steps to access the security *Utilities* menu:

1. Sign on as **QY2000** or **AM2000**.

   Note: The security utilities require high levels of user authority.

2. At the Infinium Query main menu select *Security Functions*.
3. Select *Utilities.*

   The system displays the screen illustrated in Figure 3-1.

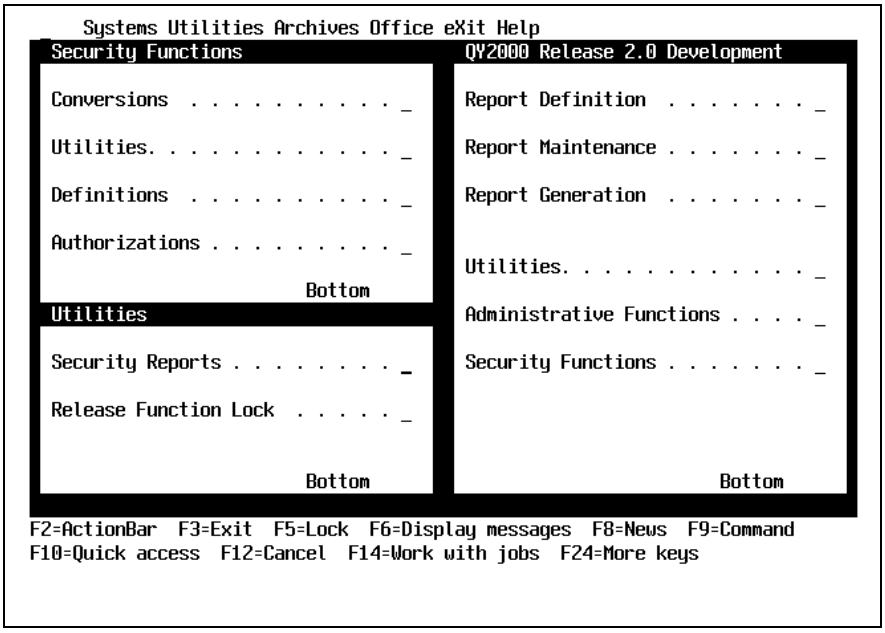


Figure 3-1: The Security Utilities menu

The following pages explain how to use these utilities.

Generating a Security Report

Choosing a Report

The following table identifies and provides a brief description of the security reports you can choose to generate.

Report	Description
User Library Authorization Report	For each user, this report identifies the user's authority level and the libraries the user is authorized to access.
User Value List Report	For each user, this report identifies the value lists that affect the user's access to specific database information. Example: A user may be limited to accessing records associated with the code for a specific company.
Infinium Level Security Report	For each Infinium Human Resources and Infinium Occupational Health user, this report identifies each company and level 1 through level 4 restriction.
Join Dependency Report	For the database you specify when you generate this report, the report identifies which file joins Infinium Query forces and which of those forced joins, if any, have been overridden from which workstation.

Refer to the separate topic about each report later in this part of the guide for more details, including illustrations of the reports' formats.

Generating the Selected Report

Perform the following steps to generate the report.

1. At the Infinium Query main menu select *Security Functions*.
2. Select *Utilities*.
3. At the *Security Utilities* menu select *Security Reports*. The system displays the *Security Reports* menu illustrated in Figure 3-2.

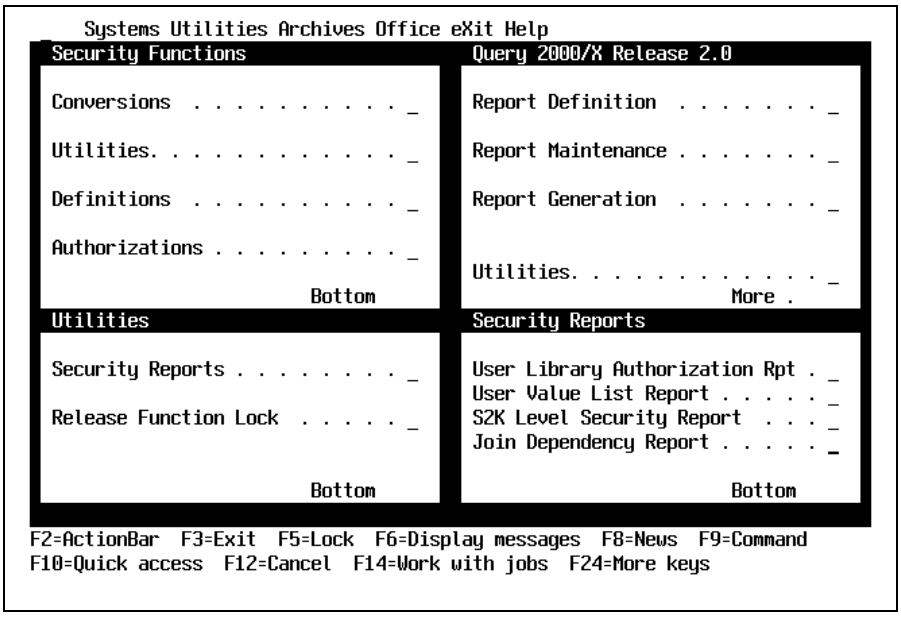


Figure 3-2: The Security Reports menu

4. At the *Security Reports* menu, select the desired report.
5. Do one of the following:

If Generating the Join Dependency Report	If Generating Any Other Report
The system prompts you for a database. Type the database library name such as HRDBFA and press Enter. The system submits the report to batch.	The system submits the report to batch. There is no separate submission screen. Go to step 6.

6. Press F14 to display the Work with Submitted Jobs screen and follow the usual steps to work with spooled file output.

Examining the User Library Authorization Report

Purpose

Examine the User Library Authorization Report to identify each user's authority level and the libraries for which that user is authorized.

The following pages provide a description and illustration of this report.

Description

This report is sorted by user. For each user, the report provides the following information.

Column	Explanation
User ID	User identifier under which the user logs on to Infinium Query.
Authority Level	Level of access authority assigned to this user, as listed in the user profile. The levels are 1 through 9, with 1 being the the highest level of authorization.
Authorized to Library: Name	Name of each library the user is authorized to access.
Authorized to Library: Level	The access level defined for this library. To access this library, the user must either have at least this level of authorization or have an authorization override defined.

Column	Explanation
Authorized to Library: Description	Brief identification of the library or libraries this user is authorized to access, such as the Infinium Human Resources database library HRDBFA.

Illustration

The following page provides an illustration of this report's format.

The illustration, designed to show the format only, has been truncated to list just a few entries.

```
QYIUSRRPT    QYTUSRRP                        Infinium Query User Library Authorization Report                      Page
1
95/02/01     16:12:19                                                                                            QY2000
User       Authority  ----------------------Authorized to Library-----------------------
ID         Level      Name        Level  Description
========== =========  ==========  =====  ================================================
AM2000          1     APDBFA066       8   AP2000 Data Base
                      DCDBFA          5   DC2000 Release 2.3 V2R2 Database Library
                      HRDBFA073       5   HR2000 Data Base
                      PRDBFA050       5   Process 5.0 programmer test data
AP2000          1     APDBFA066       8   AP2000 Data Base
                      DCDBFA          5   DC2000 Release 2.3 V2R2 Database Library
                      HRDBFA073       5   HR2000 Data Base
                      PRDBFA050       5   Process 5.0 programmer test data
BJN             5     APDBFA066       8   AP2000 Data Base
                      DCDBFA          5   DC2000 Release 2.3 V2R2 Database Library
                      HRDBFA073       5   HR2000 Data Base
                      PRDBFA050       5   Process 5.0 programmer test data
.
.
.
and so forth

                                      **********          End of Report           **********
```

Examining the User Value List Report

Purpose

Examine the User Value List Report to identify the value lists assigned to each user. Value lists are security elements used to restrict a user to certain records based on a value in a specified field. Example: An Infinium General Ledger user may be restricted to accessing records for only certain companies or accounts.

The following pages provide a description and illustration of this report.

Description

The first part of this report is sorted by user. The second part of the report is sorted by value list name.

For each user, the first part of the report provides the following information.

Column	Explanation
User ID	User identifier under which the user logs on to Infinium Query.
Library Name	Name of one or more libraries to which this user has access. **Note:** If this user has no value lists assigned, this column is blank for this user.
Value List Name	Name of the value list, if any, assigned to this user, such as **HRSEC** for Infinium Human Resources security group. **Note:** If this user has no value lists assigned, this column is blank for this user.

Column	Explanation
Description	Description of the value list identified in the previous column. **Note:** If this user has no value lists assigned, this column displays the following message: ***** No Value Lists assigned ****
OP	Operator that applies to the specified value list, as taken directly from the application database's security records by the Infinium Query conversion process. Example: **NE** for not equal. The two-character operator codes are similar to those used for Infinium Query report definition selection criteria as described in Part 3 of the *Guide to Infinium Query*.
Data	Values specified with the operator in the preceding column to indicate restrictions on the user's access. Example: **EXEC** The combination **NE EXEC** indicates that this user can access only those records for which the Security Group value is not **EXEC**.

The second part of the report is sorted by value list name. For each value list name, the second part of the report provides the following information:

Column	Explanation
Value List Name	Code name for the value list.
Description	A short description further identifying this value list.
Attachments *Library* *File* *Field*	A list of each field referenced in this value list, identified by library, file, and field names.
Field Description	A short description further identifying the field.

Illustration

The following page provides an illustration of this report's format.

The illustration, designed to show the format only, has been truncated to list selections from each section of the report.

```
SMISECRPT    SMTSECRP                          Infinium Query User Value List Report                              Page
1
95/02/01     16:13:53                                                                                          QY2000
User         Library     Value List
ID           Name        Name        Description                                OP  Data
==========  ==========  ==========  =========================================  ==  ================================================
AM2000                               *** No Value Lists assigned **
AP2000                               *** No Value Lists assigned **
BJN                                  *** No Value Lists assigned **
KMF          HRDBFA073   HRSEC       Security Groups                            NE  EXEC
             HRDBFA073                                                          NE  QYGP3
             HRDBFA073                                                          NE  QYGRP
             HRDBFA073                                                          NE  SAL
             HRDBFA073                                                          NE  2
KMM                                  *** No Value Lists assigned **
WAS                                  *** No Value Lists assigned **
.
.
.
SMISECRPT    SMTSECRP                          Infinium Query User Value List Report                              Page
3
95/02/01     16:13:53                                                                                          QY2000
Value List                                                    ---------- Attachments ---------
Name         Description                                      Library    File       Field      Field Description
==========  ================================================ ========== ========== ========== ====================================
APCO         AP2000 Default Comp                              APDBFA066  APPAG      AGCO       COMPANY
                                                              APDBFA066  APPCR      CRCO       COMPANY
                                                              APDBFA066  APPCU      CUCO       COMPANY CODE
                                                              APDBFA066  APPC9      C9CO       COMPANY
                                                              APDBFA066  APPDA      DACO       ACCOUNTING COMPANY
                                                              APDBFA066  APPDB      DBCO       COMPANY
.
.
.
APCO         AP2000 Default Comp                              APDBFA066  APPAG      AGCO       COMPANY
                                                              APDBFA066  APPCR      CRCO       COMPANY
                                                              APDBFA066  APPCU      CUCO       COMPANY CODE
                                                              APDBFA066  APPC9      C9CO       COMPANY
                                                              APDBFA066  APPDA      DACO       ACCOUNTING COMPANY
.
.
.
HRCO         HR2000 Default Co.                               HRDBFA073  PEPAP      APER       EMPLOYER NUMBER
                                                              HRDBFA073  PEPAE      AEER       EMPLOYER NUMBER
                                                              HRDBFA073  PEPAI      AIER       EMPLOYER NUMBER
                                                              HRDBFA073  PEPAI      AINTER     INTERVIEWER EMPLOYER
.
.
.
                                                              HRDBFA073  PYPYG      YGER       EMPLOYER NUMBER
HRSEC        Security Groups                                  HRDBFA073  PRPMS      PRSEC      SECURITY GROUP CODE
                                      **********              End of Report           **********
```

Examining the Application Level Security Report

Purpose

This report is primarily for diagnostic purposes rather than for routine use. The report is related to the User Value List report. For each Infinium Human Resources and Infinium Occupation Health user, the Application Level Security Report lists company and level 1 through level 4 restrictions that apply to that user.

The Application Level Security report lets you examine how application level security was converted to Query security level structure records when you ran the *Infinium Security conversion* function. This applies when, for example, an application uses levels and applies value list tests on one or more of these levels.

Example:

Suppose you set up your Infinium Human Resources system to apply user value list security rules on the company level and on the four levels within company, such as region. As a result of this setup, user NNN is granted access to all data for companies ABC and DEF. But user NNN is restricted to working with only the Southwest region for companies GHI and JKL.

At conversion, Infinium Query stores the data in this example in a data structure such as HRLVL. HRLVL refers to level-specific security information related to accessing Infinium Human Resources.

Description

The first part of this report is sorted by user. The second part of the report is sorted by structure name, such as HRLVL.

For each user, the first part of the report provides the following information:

Column	Explanation
User ID	User identifier under which the user logs on to Infinium Query
Structure Name	Name of the Infinium Query data structure in which level-specific security information about this user
Library	The database library to which the user's security restrictions apply
Description	A text description of the security level identified in the following column
Lvl	A numeric identifier of the security level. **Note:** The Infinium Query HRLVL security levels 1 through 5 correspond to the Infinium Human Resources Company and levels 1 through 4 security items. That is, Infinium Query Security Level 1 corresponds to Infinium Human Resources Company, Infinium Query Security Level 2 corresponds to Infinium Human Resources Level 1, and so forth.
Data	The value-test value for the field defined as this level in this data structure. Example: Suppose user NNN can access only Region 10 data for company ABC and Security Level 2 is defined as the field for region. The Security Level 2 entry for company ABC in this report has **`10`** in the Data column.

The following page explains the second part of this report.

The second part of the Application Level Security Report is sorted by structure name. For each Infinium Query level-specific security data structure, the second part of this report provides the following information:

Column	Explanation
Structure Name	Name of a data structure where Infinium Query stored level-specific security information, such as **HRLVL**
Description	Description of a security level, such as **Security Level 1**
Lvl	Level identifier, such as **001**
Attachments *Library* *File* *Field*	Identifiers for the library, file, and field to which the system applies the information listed in the first part of this report for this data structure
Field Description	Description of the field listed in the preceding column

Illustration

The following page provides an illustration of this report's format.

The illustration, designed to show the format only, has been truncated to list just a few entries.

```
SMISTRRPT    SMTSTRRP                          Infinium Query S2K Application Level Security Report                 Page
1
 2/01/95     16:15:15
User       Structure
ID         Name       Library     Description                          Lvl Data
======     ========== ==========  =================================== === ================================================
AM2000                            *** No Level Security assigned ***
AP2000                            *** No Level Security assigned ***
BJN                               *** No Level Security assigned ***
CLT                               *** No Level Security assigned ***
DAC        HRLVL      HRDBFA073   Security Level 1                     001  JG
                                  Security Level 1                     001  KB
                                  Security Level 2                     002 10
                                  Security Level 3                     003 910
                                  Security Level 4                     004 VPARK
                                  Security Level 5                     005 EGARG
                                  Security Level 1                     001  MB
                                  Security Level 1                     001 BM1
.
.
.
```

```
SMISTRRPT    SMTSTRRP                          Infinium Query S2K Application Level Security Report                 Page
4
 2/01/95     16:15:15
Structure                                                          ---------- Attachments ---------
Name       Description                                        Lvl Library    File       Field      Field Description
========== ================================================== === ========== ========== ========== ================================
HRLVL      Security Level 1                                   001 HRDBFA073  PRPMS      PRER       EMPLOYER NUMBER
                                    **********                 End of Report           **********
```

Examining the Join Dependency Report

Purpose

Infinium Query expects you to query certain database files only in conjunction with certain other related database files. The system therefore forces joins between these pairs of files. For additional information about joins and forced joins, see the *Guide to Infinium Query*.

Infinium Query lets you override these forced joins at the File Definition screen, as described later in Part 4 of this guide.

Examine the Join Dependency Report for a specified database to identify the following:

- The file joins required by Infinium Query for that database
- Which of those forced joins were overridden, when each was overridden, and at which workstation the override was made. The report identifies the workstation rather than the user making the change, since the user is always logged on as **QY2000**.

The following pages provide a column-by-column description and an illustration of this report.

Description

This report is sorted by file.

For each file, the report lists the following information.

Column	Explanation
File	Name of the file.
Description	Short description of this file. The description may be truncated in the case of long file descriptions.
Required Join File	Name of the file that must be joined to this file.
Join Pair 1 Field...Field...Override	The first pair of fields used to join the files, and a flag (**Y**/**N**) indicating whether this forced join has been overridden.
Join Pair 2 Field...Field...Override	The second pair of fields used to join the files, and a flag (**Y**/**N**) indicating whether this forced join has been overridden.
Last Override Date...Time...WS ID	The date, time, and workstation ID recorded for the last time an override was performed for the forced join.

Illustration

The following page provides an illustration of this report's format.

The illustration, designed to show the format only, has been truncated to list just a few entries.

```
QYIJNDRPT    QYTJNDRP                    Infinium Query Join Dependency Report For HRDBFA073                    Page
1
95/02/01     16:15:50                                                                                          QY2000
                                         Required   -------Join Pair 1-------  -------Join Pair 2-------  ------Last Override-------
File     Description                     Join File  Field    Field    Overide  Field    Field    Overide  Date     Time     WS ID
======== ============================== ========== ======== ======== =======  ======== ======== =======  ======== ======== ========
PEPAI    Personnel applicant interviews  PRPMS      PRER     AIER        N
PEPAP    Applicants File                 PRPMS      PRER     APER        Y                                 12/15/94 11:03:29 TRN1062A
PEPAT    Personnel Absences data file    PRPMS      PRER     ATER        N     PREN     ATEN        N
PEPAW    Employee automobile data        PRPMS      PRER     AWER        N     PREN     AWEN        N
PEPBU    Salary Budget Detail File       PRPMS      PRER     BUER        N     PREN     BUEN        N
PEPCI    Employee Courses Taken          PRPMS      PRER     CIER        N     PREN     CIEN        N
PEPDP    Employee Dependents File        PRPMS      PRER     DPER        N     PREN     DPEN        N
PEPED    Employee Education File         PRPMS      PRER     EDER        N     PREN     EDEN        N
PEPFN    Employee Foreign National Sala  PRPMS      PRER     FNER        N     PREN     FNEN        N
PEPHE    Safety & Health Employee Hazar  PRPMS      PRER     HEER        N     PREN     HEEN        N
PEPLF    Personnel License Fees          PRPMS      PRER     LFER        N     PREN     LFEN        N
PEPLG    Employee Log File               PRPMS      PRER     LGER        N     PREN     LGEN        N
PEPLI    Personnel Licenses              PRPMS      PRER     LIER        N     PREN     LIEN        N
PEPMC    Personnel Medical Claims        PRPMS      PRER     MCER        N     PREN     MCEN        N
PEPMS    Employee Personnel Master File  PRPMS      PRER     PEER        N     PREN     PEEN        N
PEPMST   Employee Personnel Master File  PRPMS      PRER     PEER        N     PREN     PEEN        N
PEPMV    Employee medical examinations   PRPMS      PRER     MVER        N     PREN     MVEN        N
PEPOG    Organization Master File        PRPMS      PRER     OGER        N
PEPOJ    Employee OJT Education File     PRPMS      PRER     OJER        N     PREN     OJEN        N
PEPOS    Safety and Health Master File   PRPMS      PRER     OSER        N     PREN     OSEN        N
PEPPM    Employee Path Master            PRPMS      PRER     PMER        N     PREN     PMEN        N
PEPPP    Personnel Property File         PRPMS      PRER     PPER        N     PREN     PPEN        N
PEPQC    Employee pay rate components    PRPMS      PRER     QCER        N     PREN     QCEN        N
PEPRA    Personnel recruitment costs     PRPMS      PRER     RAER        N
PEPRT    Employee development ratings    PRPMS      PRER     RTER        N     PREN     RTEN        N
PEPSW    Step code hours to date         PRPMS      PRER     SWER        N     PREN     SWEN        N
.



PYPTN    Payroll Cycle Transactions Fil  PRPMS      PRER     TNER        N     PREN     TNEN        N
PYPTP    Employee Tip Distributions Fil  PRPMS      PRER     TPER        N     PREN     TPEN        N
PYPTT    Payroll Cycle Timesheet Contro  PRPMS      PRER     TTER        N
PYPTX    W-2 Tax Master File             PRPMS      PRER     TXER        N     PREN     TXEN        N
PYPT4    T4 Workfile                     PRPMS      PRER     T4ER        N     PREN     T4EN        N
PYPT4A   T4A Workfile                    PRPMS      PRER     TAER        N     PREN     TAEN        N
PYPWC    Workers Compensation Workfile   PRPMS      PRER     WCER        N     PREN     WCEN        N
PYPWK    Time & Attendance Daily Time F  PRPMS      PRER     WKER        N     PREN     WKEN        N
PYPWL    Deductions by Levels Workfile   PRPMS      PRER     WLER        N
PYPWO    W-2 Workfile                    PRPMS      PRER     WOER        N     PREN     WOEN        N
PYPW4    401K Discrimination Test Workf  PRPMS      PRER     W4ER        N     PREN     W4EN        N
PYPW4C   401K Fund Calculations Workfil  PRPMS      PRER     W4CER       N     PREN     W4CEN       N
PYPW4K   401K Extract Tape Workfile      PRPMS      PRER     W4KER       N     PREN     W4KEN       N
                                         **********           End of Report          **********
```

Releasing Function Locks

System locks prevent simultaneous use of security functions. For example, if you run a conversion, the lock prevents another user from running that conversion or using any of the security maintenance functions.

The function lock can remain if a function is not successfully completed.

Perform the following steps to release a function lock:

1. At the Infinium Query main menu select *Security Functions*.
2. Select *Utilities*.
3. Select *Release Function Lock*.

When you select *Release Function Lock*, the system releases the lock and displays a message at the bottom of your screen, as illustrated in Figure 3-3. Press F3 twice to return to the Infinium Query main menu.

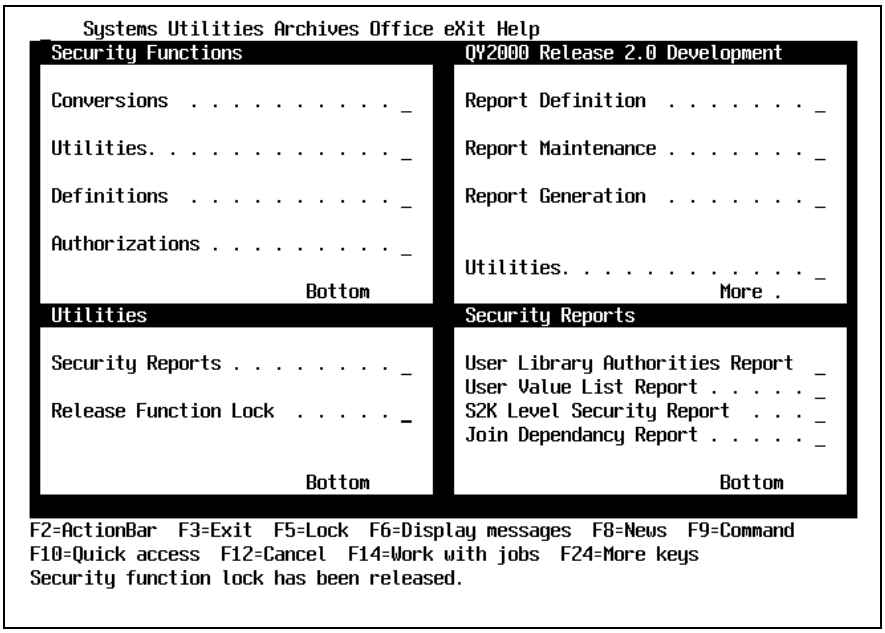
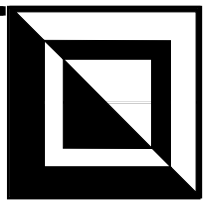


Figure 3-3: Release Function Lock Confirmation Message

Part 4



Working with Security Definitions

An Infinium Query security definition provides key Infinium Query information about a user, library, file, or field. The Infinium Query security *Definitions* menu lets you create, change, copy, delete, or display security definitions.

This part of the guide describes how to use the *Definitions* menu options.

Note: You must sign on as **`QY2000`** to use any of these options.

The following table summarizes the tasks covered in this part of the guide.

Accessing the Security *Definitions* Menu

Perform the following steps to access the security *Definitions* menu:

1. At the Infinium Query main menu select *Security Functions*.
2. Select *Definitions*. The system displays the *Definitions* menu.

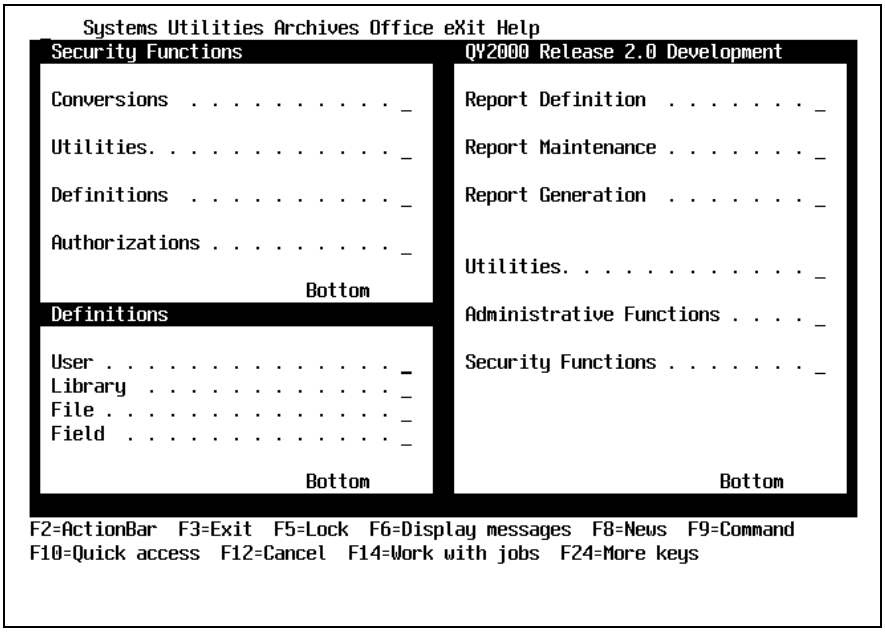


Figure 4-1: Security Definitions menu

The *Definitions* menu also includes *Value List* if you are using Infinium Query/X (Infinium Query/Extended), which allows conversion and querying of databases not developed by Infinium. The only value list definitions you can work with in this function are those for non-Infinium databases.

The following pages provide detailed instructions for using the options on this menu.

Working with User Definitions

An Infinium Query user definition contains key information about an Infinium Query user. A user definition consists of a user ID, a description such as the user's name, and the user's authority level.

Caution: The system refreshes this information from the Infinium Application Manager profile at each conversion. Infinium therefore recommends that you make authorization changes through the security *Authorizations* menu rather than through the *Definitions* menu.

Perform the following steps to work with user definitions:

1. At the Security *Definitions* menu select *User*. The system displays the User Definitions screen.

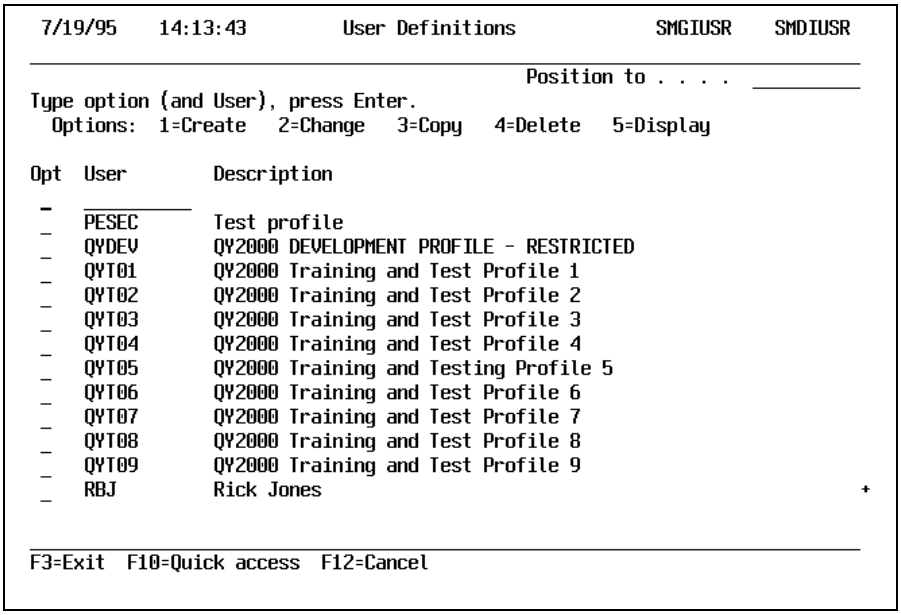


Figure 4-2: User Definitions screen

Note: This screen lists all your Infinium Query users.

2. If necessary, press PgDn to page through the list to find the user record you want to work with. Then type one of the following numbers in the *Opt* field next to that user's entry.

Value	Explanation
2	To change an existing user definition
3	To copy an existing user definition
4	To delete an existing user definition
5	To display an existing user definition

Note: You can also create a new user definition. Type **1** in the first row of the *Opt* column and a user ID in the first row of the *User* column. Refer to the Warning on the next page.

3. Press Enter to continue.

   The system displays the applicable User Definitions screen, such as the Change User Definition screen for the change function.

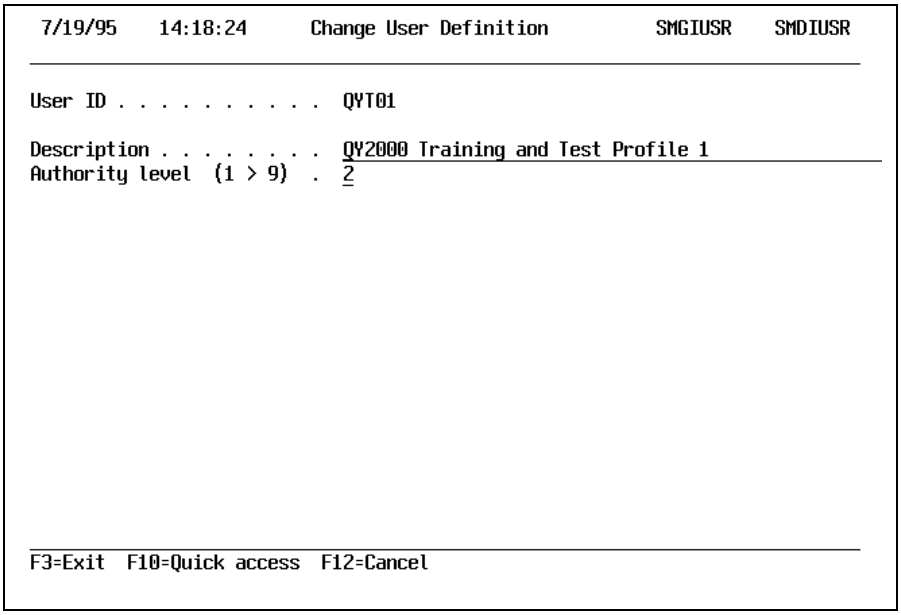


Figure 4-3: Change User Definition screen

4. Do one of the following at the user definition screen, depending on the task you are performing.

Task	Action
Creating	Type the user's description and authority level.
Changing	Type a new description, authority level, or both.
Copying	Type a new user ID. The description and authority level field values default from the record you copied. You can type a different description or authority level if applicable.
Deleting	Press Enter to confirm the deletion or press F12 to cancel the deletion. If you press Enter, the system displays a message that the entry is marked for deletion.
Displaying	View the displayed data.

Warning:

If you add a new user definition, that user has full authority to all files that are applicable for the authority level you specify in the new definition.

Infinium therefore recommends that you add all user profiles in Infinium Application Manager to maintain product security.

Note: All changes made through the *Definitions* menu options are overridden when you run a conversion. Changes made through the *Definitions* menu are only active until the next conversion.

5. When done, do one of the following to return to the Infinium Query main menu.

Task	Exit Steps
Creating, copying, changing, or deleting a definition	Press F3 repeatedly to exit to the Infinium Query main menu and confirm any changes, or press F12 repeatedly to cancel and return to the Infinium Query main menu.
Displaying a definition	Press F12 repeatedly to return to the Infinium Query main menu.

Working with Library Definitions

An Infinium Query library definition contains key Infinium Query information about an application library including the library name, a description of the library, and the library's defined authority level.

Perform the following steps to work with Library Definitions:

1. At the Security *Definitions* menu select *Library*.
   The system displays the Library Definitions screen.

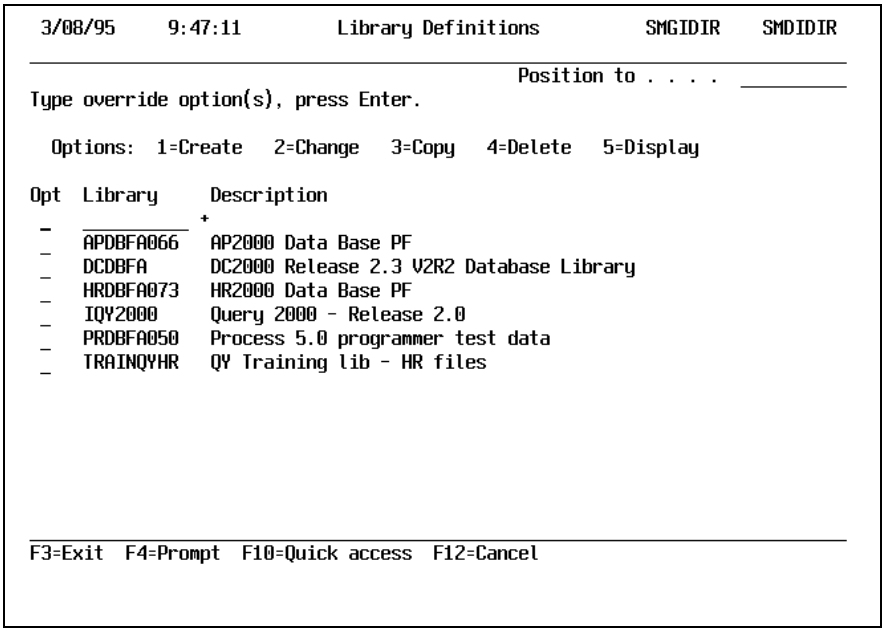


Figure 4-4: Library Definitions screen

Note: This screen lists all libraries on your system that are available to your Infinium Query users. These libraries are the database libraries of applications for which Infinium Query security conversions have been run on your system.

2. If necessary, press PgDn to page through the list to find the library definition you want to work with. Type one of the following numbers in the *Opt* field next to that library's entry.

Value	Explanation
2	To change an existing library definition
3	To copy an existing library definition
4	To delete an existing library definition
5	To display an existing library definition

Note: You can also create a new library definition. Type **1** in the first row of the *Opt* column and a library name in the first row of the *Library* column. Infinium strongly recommends, however, that you use security conversion to establish all definitions. This is particularly important for Infinium applications for which you use the *Run Infinium Conversion* function.

3. Press Enter to continue.

   The system displays the applicable Library Definitions screen, such as the Change Library Definition screen for the change function.

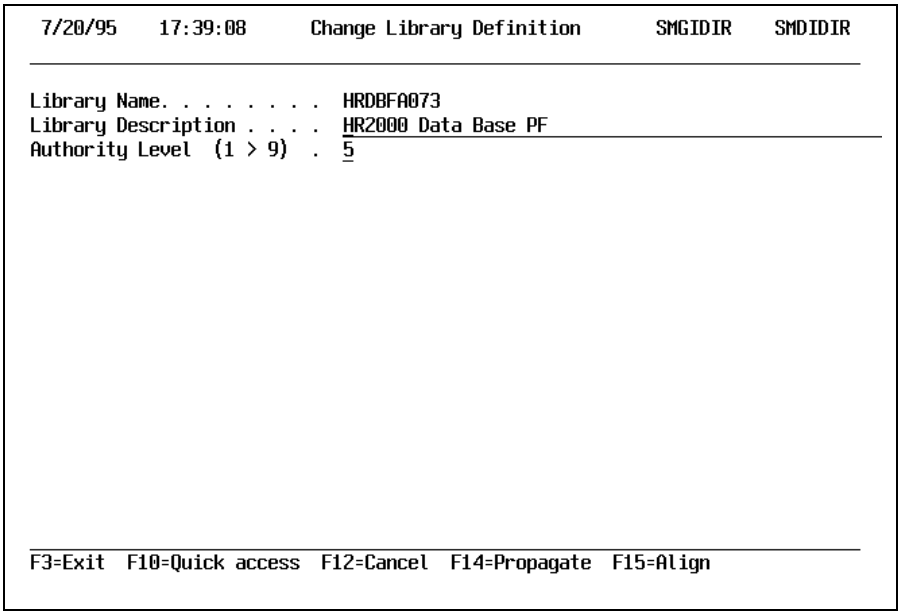


Figure 4-5: Change Library Definition screen

4. Do one of the following at the Library Definition screen, depending on the task you are performing.

Task	Action
Creating	Type the library's description and authority level.
Changing	Type a new description, authority level, or both.
Copying	Type a new library name. The description and authority level field values default from the record you copied. You can type a different description or authority level if applicable.
Deleting	Press Enter to confirm the deletion or press F12 to cancel the deletion. If you press Enter, the system displays a message that the entry is marked for deletion. **Note:** If restrictions prevent deletion, the system displays one of the following messages: • **`File definitions dependencies prevent completion of request`**. You must first delete all the definitions for the files included in this library. • **`Library authorization dependencies prevent completion of request`**. You must first use the *Authorizations* function to delete the related authorization record or records for this library.
Displaying	View the displayed data.

Note: All changes made through the *Definitions* menu option are overridden when you run a conversion. Changes made through the *Definitions* menu are only active until the next conversion.
When you make changes, you can also use the following function keys.

Key	Use
F14	If you change the library's authority level (from **5** to **4**, for example), pressing this Propagate key tells the system also to find all files and fields in that library with the library's prior level (such as **5**) and change their authority level also to the library's new level (such as **4**).
F15	Pressing this Align key tells the system to change all files and fields within this library to current authority level specified for this library.

Infinium recommends using reconversion rather than using these keys.

5. When done with the Change Library Definition function, do one of the following to return to the Infinium Query main menu.

Task	Exit Steps
Creating, copying, changing, or deleting a definition	Press F3 repeatedly to exit to the Infinium Query main menu and confirm any changes, or press F12 as often as necessary to cancel and return to the Infinium Query main menu.
Displaying a definition	Press F12 repeatedly to return to the Infinium Query main menu.

Working with File Definitions

An Infinium Query file definition contains key information about an application file, including the library name, file name, a description of the file, and an authority level.

Perform the following steps to work with file definitions:

1. At the *Security Definitions* menu select *File*.

   The system displays the Select Library screen.

```
 2/14/95    11:02:23        Select Library              SMGITBL    SMDITBL

                                                Position to . . . .

Type any character to select library(s), press Enter.

Sel  Library     Description
 _   APDBFA066   AP2000 Data Base PF
 _   DCDBFA      DC2000 Release 2.3 V2R2 Database Library
 _   HRDBFA073   HR2000 Data Base PF
 _   PRDBFA050   Process 5.0 programmer test data
 X   TRAINQYHR   QY Training lib - HR files

F3=Exit  F10=Quick access  F12=Cancel
```

Figure 4-6: Select Library screen

Note: This screen lists all libraries on your system that are available to Infinium Query users. These are the database libraries of applications for which Infinium Query security conversions have been run on your system.

2. If necessary, press PgDn to page through the list to find the library to which the file belongs. Select the library you want to work with by typing any character in the *Sel* column next to that library's entry.
3. Press Enter to display the File Definitions screen for that library, listing the library's files.

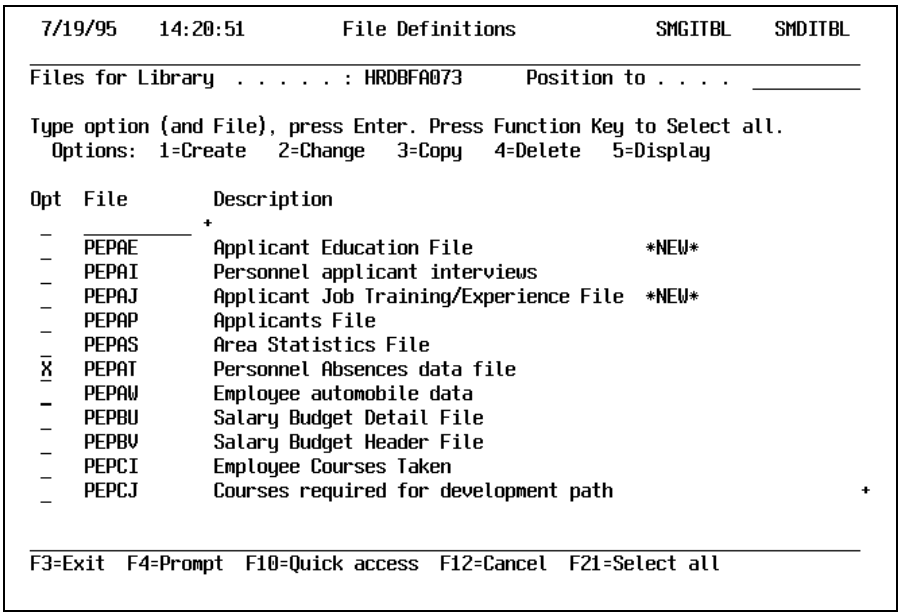


Figure 4-7: File Definitions screen

4. If necessary, press PgDn to page through the list to find the file record you want to work with. Type one of the following in the *Opt* field next to that file's entry.

Value	Explanation
2	To change an existing file definition
3	To copy an existing file definition
4	To delete an existing file definition
5	To display an existing file definition

Note: To create a new file definition, type **1** in the first row of the *Opt* column and a file name in the first row of the *File* column. This function is only for Infinium Query/X users working with non-Infinium database application libraries they have converted for Infinium Query/X. Do not type **1** for Infinium application files.

5. Press Enter to continue.

   The system displays the applicable file definitions screen, such as the Change File Definition screen for the change function.

```
 7/19/95    14:23:47       Change File Definition          SMGITBL    SMDITBL
 ____________________________________________________________________________

 Library Name. . . . . .  HRDBFA073
 File Name . . . . . .  PEPAT
 File Description. . . . . .  Personnel Absences data file
 Authority Level  (1 > 9)  .  4

 Join Dependency File  . . .  PRPMS
                                                          Override
                                                        0=No, 1=Yes
   Join Field pair #1  . . .  ATER          PRER             0
   Join Field pair #2  . . .  ATEN          PREN             0
 ____________________________________________________________________________
 F3=Exit  F10=Quick access  F12=Cancel  F14=Propagate  F15=Align
```

Figure 4-8: Change File Definition screen

Note: The *Join Dependency File* and *Join Field Pair* fields are used only for Infinium Human Resources and Infinium Occupational Health files with forced joins, as described later in this task topic. For more information about forced joins, refer to Part 4 of the *Guide to Infinium Query*.

WARNING

Forced joins ensure that Infinium Human Resources and Infinium Occupational Health security is applied. If you override the forced joins, the security for these applications is not fully applied for query reports, and users may have access to data for which they are not authorized.

6. Do one of the following at the File Definition screen, depending on the task you are performing.

Task	Action
Creating	Type the file's description and authority level.
Changing	Refer to the information on changing a file definition after this table.
Copying	Type a new library name. The description and authority level field values default from the record you copied. You can type a different description or authority level if applicable.
Deleting	Press Enter to confirm the deletion or press F12 to cancel the deletion. If you press Enter, the system displays a message that the entry is marked for deletion. **Note:** If restrictions prevent deletion, the system displays one of the following messages: • **`Field definitions dependencies prevent completion of request.`** You must first delete all the definitions for the fields included in this file. • **`File authorization dependencies prevent completion of request.`** You must first use the *Authorizations* function to delete the related authorization record or records for this file.
Displaying	View the displayed data.

Changing a File Definition

Changing a file definition consists of updating one or more of the fields on the Change File Definition screen. This screen lets you edit the file's description and authority level, and lets you override one or both of forced-join field pairs, if any. Forced joins are file-join definitions automatically assigned by the Infinium Query system.

The following paragraphs explain how to use the fields on this screen.

Library Name

This display-only field identifies the library you selected in step 2.

File Name

This display-only field identifies the file you selected in step 4.

File Description

Type a new description if applicable.

Authority Level (1 > 9)

Type a new authority level if applicable.

Join Dependency File

Join dependency fields apply only to files for Infinium HR/PY, Infinium Occupational Health, or their modules like Infinium Human Resources, Infinium Payroll, or Infinium Occupational Health.

The *Join Dependency File* field displays the name of the file to which the file you are defining must be joined. For a Infinium Human Resources library, the field value is **PRPMS**. For an Infinium Occupational Health library, the field value is **EMPHM**. You cannot edit this field.

Join Field pair #1

Type **0** to accept the forced join or **1** to override and not force the join.

Join Field pair #2

Type **0** to accept the forced join or **1** to override and not force the join.

If you override the forced joins, users designing reports that use this file are not required to use the related join-dependency file for those reports.

Note: All changes made through the *Definitions* menu option are overridden when you run a conversion. Changes made through the *Definitions* menu are only active until the next conversion. Refer to Part 4 of the *Guide to Infinium Query* for more information about forced joins.

7. When you make changes, you can also use the following keys.

Key	Use
F14	If you change the file's authority level (such as from **5** to **4**), you can press this Propagate key to change any of the file's fields that have the file's prior authority level (such as **5**) to the new level (such as **4**).
F15	Pressing this Align key changes the authority level on all fields in this file to the level currently assigned to this file.

Infinium recommends using reconversions rather than using these keys.

8. When done with file definition, do one of the following to return to the Infinium Query main menu.

Task	Exit Steps
Creating, copying, changing, or deleting a definition	Press F3 repeatedly to exit to the Infinium Query main menu and confirm any changes, or press F12 repeatedly to cancel and return to the Infinium Query main menu.
Displaying a definition	Press F12 repeatedly to return to the Infinium Query main menu.

Working with Field Definitions

An Infinium Query field definition consists of a library name, file name, field name, an Infinium Query description of the field, and an authority level.

Perform the following steps to work with field definitions:

1. At the security *Definitions* menu select *Field*.

   The system displays the Select Library screen, illustrated earlier in Figure 4-6.

2. If necessary, press PgDn to page through the list to find the library that contains the file with the field you want. Select the library by typing any character in the *Sel* column next to that library's entry.

3. Press Enter to display the Select File screen for that library.

```
 7/19/95    14:25:44          Select File                  SMGICOL    SMDICOL

Library: HRDBFA073                                Position to . . . .  _________

Type any character to select file(s), press Enter.

Sel  File        Description
 _   PEPAE       Applicant Education File                 *NEW*
 _   PEPAI       Personnel applicant interviews
 _   PEPAJ       Applicant Job Training/Experience File   *NEW*
 _   PEPAP       Applicants File
 _   PEPAS       Area Statistics File
 X   PEPAT       Personnel Absences data file
 _   PEPAW       Employee automobile data
 _   PEPBU       Salary Budget Detail File
 _   PEPBV       Salary Budget Header File
 _   PEPCI       Employee Courses Taken
 _   PEPCJ       Courses required for development path
 _   PEPCK       Personnel Course Master                                      +


F3=Exit  F10=Quick access  F12=Cancel
     _
```

Figure 4-9: Select File screen

4. If necessary, press PgDn to page through the list to find the file containing the field you want to work with. Type any character in the *Sel* column next to that file entry to select the file.
5. Press Enter to display the Field Definitions screen for that file.

```
 7/19/95    14:27:14          Field Definitions           SMGICOL    SMDICOL

Library: HRDBFA073        File: PEPAT         Position to . . . .  _________

Type option (and Field), press Enter.  Press Function Key to select all.
  Options:  1=Create   2=Change   3=Copy   4=Delete   5=Display
            8=Attach/Detach Value List

Opt  Field       Description
 _   _________ +
 _   ATABS       ABSENCE CODE
 _   ATCOMM      COMMENT
 _   ATCSFT      SHIFT CODE
 _   ATDATE      ABSENCE DATE -EDITED
 _   ATDATH      ABSENCE DATE - EDITED
 _   ATDAT8      ABSENCE DATE - 8 DIGIT
 _   ATDAY       DAY NUMBER OF WEEK
 2   ATEN        EMPLOYEE NUMBER
 -   ATER        EMPLOYER NUMBER
 _   ATHRS       HOURS ABSENT
 _   ATJOB       JOB CODE                                                   +

F3=Exit  F4=Prompt  F10=Quick access  F12=Cancel  F21=Select all
```

Figure 4-10: Field Definitions screen

This screen lists all fields included in the file you selected.

6. If necessary, press PgDn to page through the list to find the field. Type one of the following in the *Opt* field next to that field's entry.

Value	Explanation
2	To change the field's definition
3	To copy the field's definition
4	To delete the field's definition
5	To display the field's definition
8	To attach a value list to the field's definition or detach a value list from the field's definition

Note: To create a new field definition for a non-Infinium application field converted to Infinium Query/X, type **1** in the first

row of the *Opt* column and a field name in the first row of the field column. You cannot create a new field definition record for Infinium database application fields.

7. Press Enter to continue.

   The system displays the applicable field definitions screen, such as the Change Field Definition screen for the change function.

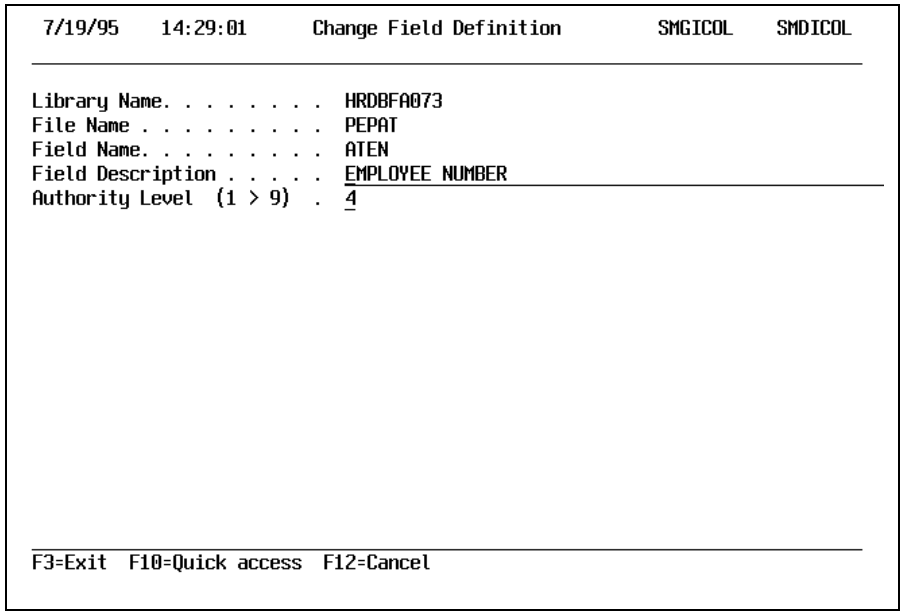


Figure 4-11: Change Field definition screen

8. At the Change Field Definition screen, perform one of the actions described in the following table, depending on the task you are performing.

Task	Action
Creating	Type the field's description and authority level.
Changing	Type a new description or authority level or both.
Copying	Type a new field name. The description and authority level default in from the record you copied. You can type a different description or authority level if applicable.

Task	Action
Deleting	Press Enter to confirm the deletion or press F12 to cancel the deletion. If you press Enter, the system displays a message that the entry is marked for deletion. **Note:** If restrictions prevent deletion, the system displays the following message: **`Field authorization dependencies prevent completion of request.`** You must first delete the related authorization record or records for this field.
Displaying	View the displayed data.
Attaching /detaching a value list	Type the name of the value list to be attached to or detached from this field. For more information about value lists, refer to the next topic in this part of the guide.

Note: All changes made through the *Definitions* menu are overriden when you run a conversion. Changes made through the *Definitions* menu are only active until the next conversion.

9. When done, do one of the following to return to the Infinium Query main menu.

Task	Exit Steps
Creating, copying, changing, or deleting a definition, or attaching /detaching a value list	Press F3 repeatedly to exit to the Infinium Query main menu and confirm any changes, or press F12 repeatedly to cancel and return to the Infinium Query main menu.
Displaying a definition	Press F12 repeatedly to return to the Infinium Query main menu.

Working with Infinium Query/X Value List Definitions

An Infinium Query/X value list ensures data security in a non-Infinium application if applied during use of Infinium Query/X. The value list identifies value tests associated with a specific field. The test can limit the user's access to records that contain one of the specified values in that field. Alternatively, the test can specify that the user be excluded from records that contain one of the specified values in that field.

A value list definition specifies the value list's name and description and the field's data type, length, and number of decimal positions.

Caution: Perform this task only for non-Infinium applications. The *Infinium Security Conversion* function handles value lists for Infinium applications without further work on your part.

Use the following functions for non-Infinium value lists.

Task	Function
Create a Value List Definition	*Definitions* menu's *Value List* option
Specify or change the field with which the value list is associated, or detach the value list from the field	*Definitions* menu's *Field* option (use the Attach/Detach feature) or *Value List* option; refer to the Working with Field Definitions subtopic in this part of the guide for details.
Create the list of values that define which records a user can access	*Authorizations* menu's *User* option; refer to the Working with Infinium Query/X Value List Authorizations subsection in Part 5 of this guide for details.

The following pages provide instructions for using the *Definitions* menu's *Value List* option.

1. At the security *Definitions* menu, select *Value List*.
   The system displays the Value List Definitions screen.

Note: The following screens are for illustration only. Perform these steps only for non-Infinium database applications.

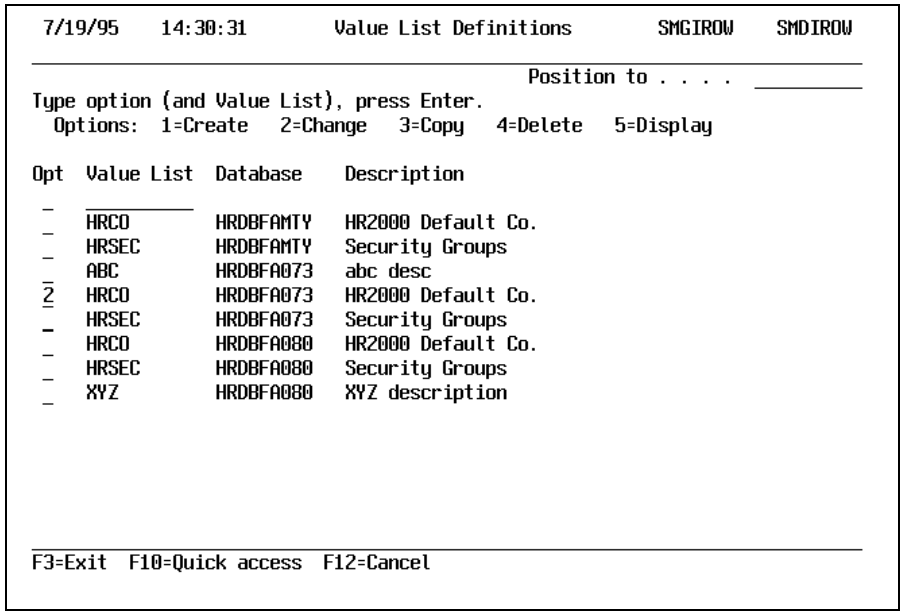


Figure 4-12: Value List Definitions screen

2. If necessary, press PgDn to page through the list to find the value list with which you want to work. Type one of the following in the *Opt* field next to that value list's entry.

Value	Explanation
2	To change the value list's definition
3	To copy the value list's definition
4	To delete the value list's definition
5	To display the value list's definition

Note: To create a new definition, type **1** at the top of the *Opt* column and a value list name at the top of the *Value List* column.

3. Press Enter to continue. The system displays the applicable value list definition screen, such as the Change Value List Definition screen for the change function.

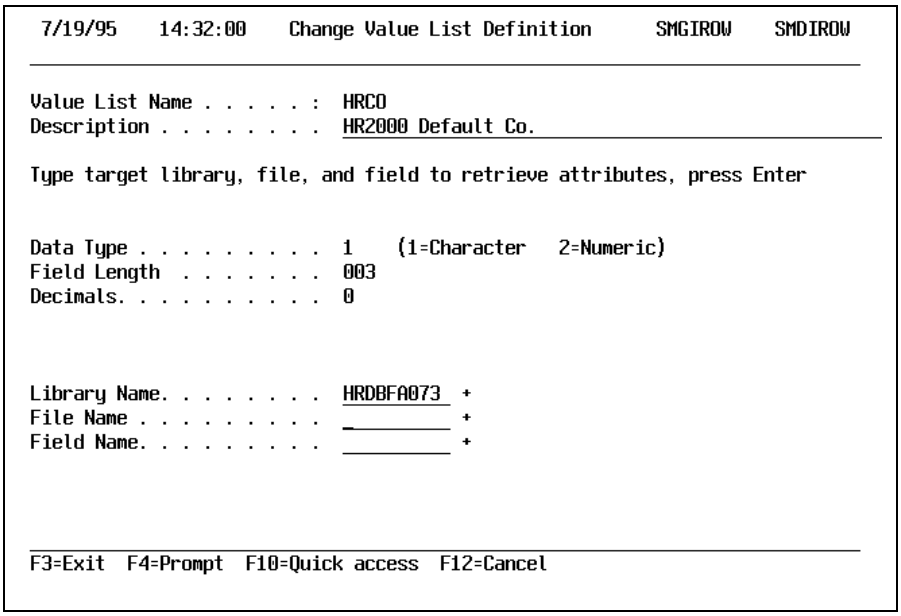


Figure 4-13: Change Value List Definition screen

Note: The system displays the *Library Name*, *File Name*, and *Field Name* fields only for the create and change functions.

4. Do one of the following at the Value List Definitions screen, depending on the task you are performing.

Task	Action
Creating	Type the value list's description, and specify the associated field's library, file, and field name to retrieve the field's attributes in the *Data Type*, *Field Length*, and *Decimals* fields.
Changing	Type a new description, or new target library, file and field names, or both, if applicable.
Copying	Type a new value list name. The description field defaults in from the record you copied. You can type a different description.
Deleting	Press Enter to confirm, or F12 to cancel, the deletion.
Displaying	View the displayed data.

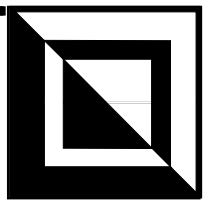
Note: All changes made through the *Definitions* menu are overridden when you run a conversion. Changes made through the *Definitions* menu are only active until the next conversion.

5. When done, do one of the following to return to the Infinium Query main menu.

Task	Exit Steps
Creating, copying, changing, or deleting a definition	Press F3 repeatedly to exit to the Infinium Query main menu and confirm any changes, or press F12 repeatedly to cancel and return to the Infinium Query main menu.
Displaying a definition	Press F12 repeatedly to return to the Infinium Query main menu.

Notes

Part 5



Working with Security Authorizations

The authority level specified in your Infinium Application Manager user profile determines your ability to access a library, file, or field. An Infinium Query security authorization allows you to grant, revoke, or override a user's authority to access a library, file, or field.

This part of the guide describes how to use the Infinium Query *Authorizations* menu options.

Note: You must sign on as **`QY2000`** to use any of these options.

The following table summarizes the tasks covered in this part of the guide.

Note: Authorization overrides are not overwritten when you perform a subsequent security conversion.

Accessing the Security Authorizations Menu

Perform the following steps to access the *Security Authorizations* menu:

1. At the Infinium Query main menu select *Security Functions*.
2. Select *Authorizations*. The system displays the *Authorizations* menu.

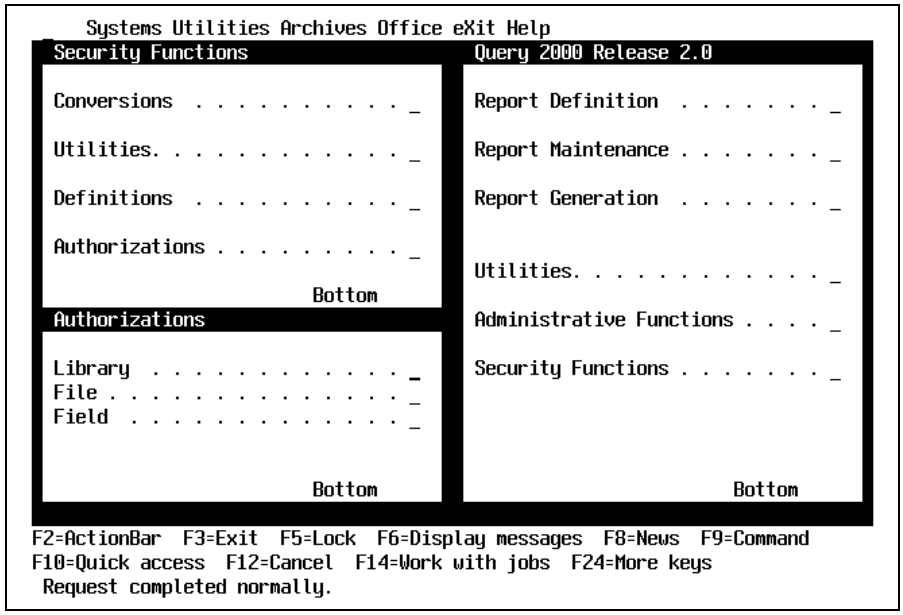


Figure 5-1: Security Authorizations menu

If you are using Infinium Query/X, this menu also includes the *Value List* authorization option, which lets you grant a user authority to access data based on a value list or modify the data values in the value list.

The following pages provide detailed instructions for using the options on this menu.

Working with Library Authorizations

An Infinium Query library authorization is an application feature that lets you modify a particular user's authority to access a particular library. This lets you provide library access to a user whose default authorization level number, which was converted from the user's Infinium Application Manager user profile, is higher than the library's authorization level number.

For information about security conversions, refer to Part 2 of this guide.

A user's default authorization to access a library is based on the combination of the user's authorization level and the library's authorization level. If the user's level is the same number or a lower number than the library's level, the user can access the library.

Examples:

- Sam's Infinium Application Manager profile assigns him level 5.
- Library X has level 4. Sam cannot access this library.
- Library Y has level 5. Sam can access this library.

Perform the following steps to work with Library Authorizations:

1. At the Security *Authorizations* menu select *Library*. The system displays the Select User ID screen.

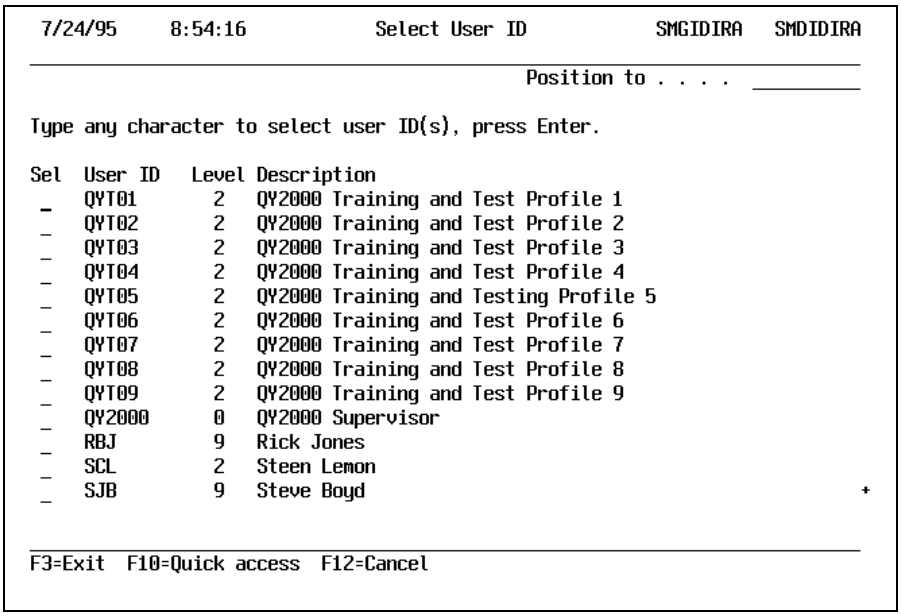


Figure 5-2: Select User ID screen

This screen lists all Infinium Query users and the authority level assigned to each of these users.

2. If necessary, PgDn through the list to find the user whose library authorization is to be modified. Select the user by typing any character in the *Sel* column next to the user ID and pressing Enter.

   The system displays the Library Authority screen.

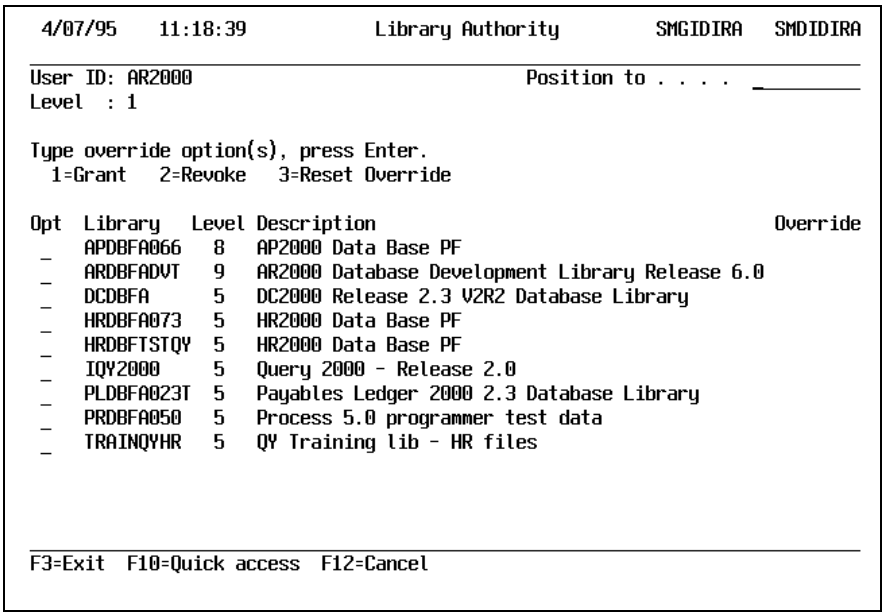


Figure 5-3: Library Authority screen

This screen lists all the libraries available for Infinium Query use, the authority level a user must have to access that library, and a description of the library. The screen also specifies the authority level override, if any, that applies to this library for this user.

Note: In the upper left corner of this screen, the system displays the User ID and authority level assigned to the user you selected.

3. Type one of the following in the *Opt* field next to a library name:

Value	Explanation
1	Grant this user access to this library, overriding the default authority.
2	Restrict this user from access to this library.
3	Reimplement the default access authority that applies to this user for this library.

4. Press F3 to exit to the Exit Options window, type **1**, and press Enter to confirm your changes.
5. Press F3 again to exit to the Security *Authorizations* menu.

Working with File Authorizations

Infinium Query file authorization is an application feature that lets you modify a particular user's authority to access a particular file. This lets you provide file access to a user whose default authorization level number, which was converted from the user's Infinium Application Manager user profile, is higher than the file's authorization level number.

For information about security conversions, refer to Part 2 of this guide.

A user's default authorization to access a file is based on the combination of the user's authorization level and the file's authorization level. If the user's level is the same number or a lower number than the file's level, the user can access the file.

Note: To access a file, the user must also be authorized to access the library in which that file resides.

Perform the following steps to work with File Authorizations:

1. At the Security *Authorizations* menu select *File*. The system displays the Select User ID screen illustrated earlier in Figure 5-2.
2. If necessary, PgDn through the list to find the user record to be modified. Select the record by typing any character in the *Sel* column next to the user ID and pressing Enter.

   The system displays the Select Library screen.

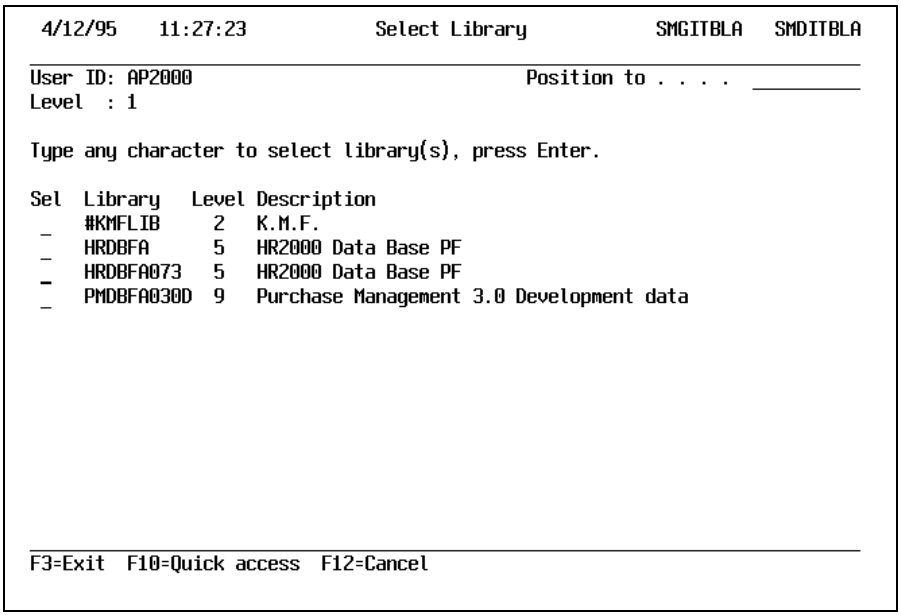


Figure 5-4: Select Library screen

This screen lists all libraries available for Infinium Query use, the authority level a user must have to access that library, and a description of the library.

Note: At the top left of this screen, the system displays the User ID and authority level assigned to the user you selected in step 2.

3. Type any character in the *Sel* column next to the library that contains the file you want to work with.

   The system displays the File Authority screen.

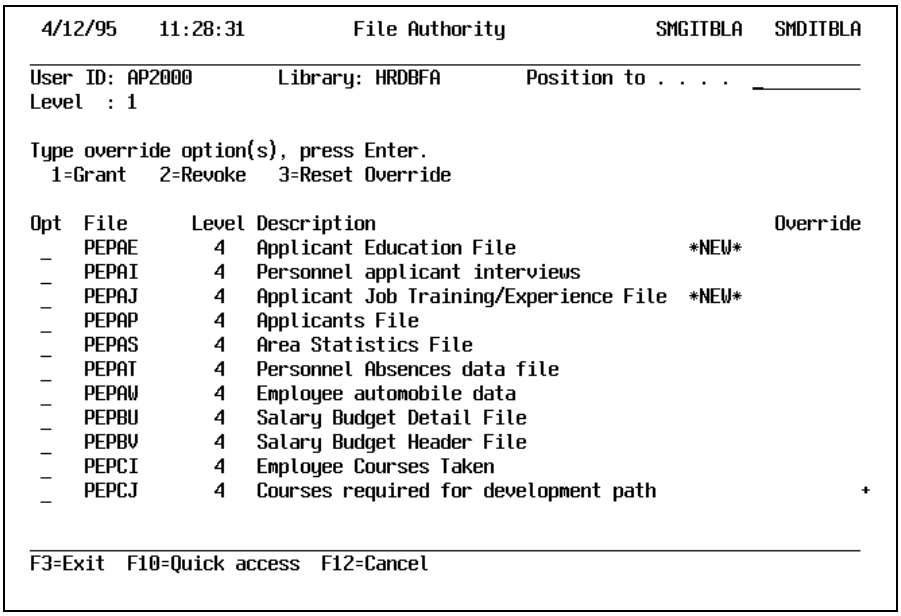


Figure 5-5: File Authority screen

This screen lists all the files in the application library you selected, the authority level needed to access that file, and a description of the file. The screen also specifies the authority level override, if any, that applies to this file for this user.

4. Type one of the following in the *Opt* field next to the file's name.

Value	Explanation
1	To grant this user access to this file, overriding the default authority.
2	To restrict this user from access to this file.
3	To reimplement the default access authority that applies to this user for this file.

5. Press F3 to exit to the Exit Options window, type **1**, and press Enter to confirm your changes.
6. Press F3 again to exit back to the Security *Authorizations* menu.

Working with Field Authorizations

Infinium Query field authorization is an application feature that lets you modify a particular user's authority to access a particular field. This lets you provide field access to a user whose default authorization level number, which was converted from the user's Infinium Application Manager user profile, is higher than the field's authorization level number.

For information about security conversions, refer to Part 2 of this guide.

A user's default authorization to access a field is based on the combination of the user's authorization level and the field's authorization level. If the user's level is the same number as or a lower number than the field's level, the user can access the field.

Note: To access a field, the user must also have the authority to access the library and the file in which the field resides.

Perform the following steps to work with Field Authorizations:

1. At the Security *Authorizations* menu, select *Field*. The system displays the Select User ID screen illustrated earlier in Figure 5-2.
2. If necessary, page down through the list to find the user whose field authorizations you want to work with. Select the user by typing any character in the *Sel* column next to the user ID and press Enter.

   The system displays the Select Library screen illustrated earlier in Figure 5-4.
3. Type any character in the *Sel* column next to the library that contains the file and fields you want to work with. The system displays the Select File screen.

```
 4/12/95    11:29:32            Select File              SMGICOLA   SMDICOLA
_____________________________________________________________________________
User ID: AP2000        Library: HRDBFA        Position to . . . .  __________
Level  : 1

Type any character to select file(s), press Enter.

Sel  File      Level Description
 _   PEPAE       4   Applicant Education File               *NEW*
 _   PEPAI       4   Personnel applicant interviews
 _   PEPAJ       4   Applicant Job Training/Experience File  *NEW*
 _   PEPAP       4   Applicants File
 _   PEPAS       4   Area Statistics File
 _   PEPAT       4   Personnel Absences data file
 _   PEPAW       4   Employee automobile data
 _   PEPBU       4   Salary Budget Detail File
 _   PEPBV       4   Salary Budget Header File
 _   PEPCI       4   Employee Courses Taken
 _   PEPCJ       4   Courses required for development path
 _   PEPCK       4   Personnel Course Master                                +


_____________________________________________________________________________
F3=Exit  F10=Quick access  F12=Cancel
```

Figure 5-6: Select File screen

4. Type any character in the *Sel* column next to the name of the file that contains the field or fields you want to work with. Then press Enter. The system displays the Field Authority screen.

```
 4/12/95    11:30:38          Field Authority            SMGICOLA   SMDICOLA
_____________________________________________________________________________
User ID: AP2000        Library: HRDBFA        Position to . . . .  __________
Level  : 1             File   : PEPDP

Type override option(s), press Enter.
  1=Grant   2=Revoke   3=Reset Override

Opt  Field     Level Description                                    Override
 _   DPADR1      4   ADDRESS LINE 1
 _   DPADR2      4   ADDRESS LINE 2
 _   DPADR3      4   ADDRESS LINE 3
 _   DPDAG       4   DEPENDENT AGE
 _   DPDBE       4   D O B EDITED
 _   DPDBH       4   D O B HYF
 _   DPDB8       4   D O B 8 DIGT
 _   DPDNM       4   DEPENDENT NAME
 _   DPEN        4   EMPLOYEE
 _   DPER        4   EMPLOYER
 _   DPREL       4   RELATIONSHIP                                      +


_____________________________________________________________________________
F3=Exit  F10=Quick access  F12=Cancel
```

Figure 5-7: Field Authority screen

5. Type one of the following in the *Opt* field next to a field name.

Value	Explanation
1	To grant this user access to this field, overriding the default authority.
2	To restrict this user from access to this field.
3	To reimplement the default access authority that applies to this user for this field.

6. Repeat for additional fields if applicable.

   Note: If you know the exact name of a target field, such as DPEN, you can type a field name in the *Position to* field at the top right of the screen and then press Enter to move directly to that field.

7. When done working with these fields, press F3 to exit to the Exit Options window, type **1**, and press Enter to save your changes.

8. Press F3 again to exit back to the Security *Authorizations* menu.

Working with Infinium Query/X Value List Authorizations

An Infinium Query/X value list ensures data security in a non-Infinium application is applied during use of Infinium Query/X. The list identifies value tests associated with a specific field for a user. The test can limit the user's access to records that contain one of the specified values in that field. Alternatively, the test can specify that the user be excluded from records that contain one of the specified values in that field.

A value list authorization record contains the tests included in the specified value list for the specified user.

Caution: Perform this task only for non-Infinium applications. The *Infinium Security Conversion* function performed with the ***USERS** option modifies value lists for Infinium application users without further work on your part.

Use the following functions for non-Infinium value lists.

Task	Function
Create a Value List Definition	*Definitions* menu's *Value List* option; refer to Part 4 of this guide for details.
Specify or change the field with which the value list is associated, or detach the value list from the field	*Definitions* menu's *Field* option (use the Attach/Detach feature) or *Value List* option; refer to Part 4 of this guide for details.
Create the list of values that define which records a user can access	*Authorizations* menu's *User* option

The following pages provide instructions for using the *Definitions* menu's *Value List* option.

1. At the Security *Authorizations* menu, select *Value List*.
   The system displays the Select User ID screen illustrated earlier in Figure 5-2.

2. If necessary, page down through the list to find the applicable user. Select that user by typing any character in the *Sel* column next to the user ID and press Enter.

   When you select a user, the system displays the Select Value List screen, listing value lists associated with that user.

```
 7/10/95    17:35:53          Select Value List            SMGIROWA   SMDIROWA
_____________________________________________________________________________
User ID: QYT01                                  Position to . . . .  _________

Type option(s), press Enter.
  Options:  3=Copy to user ID  5=Assign values

Sel  Value List   Description
 _    HRCO         HRDBFAMTY   HR2000 Default Co.
 _    HRSEC        HRDBFAMTY   Security Groups
 _    ABC          HRDBFA073   abc desc
 _    HRCO         HRDBFA073   HR2000 Default Co.
 _    HRSEC        HRDBFA073   Security Groups
 _    HRCO         HRDBFA080   HR2000 Default Co.
 _    HRSEC        HRDBFA080   Security Groups
 _    XYZ          HRDBFA080   XYZ description




_____________________________________________________________________________
F3=Exit  F10=Quick access  F12=Cancel
```

Figure 5-8: Select Value List screen

   The system displays the user's ID at the top left of this screen.

3. Type one of the following in the *Sel* field next to a value list:

Value	Explanation
3	To copy a value list authorization for another user. The target user inherits the authorities and data associated with the copied value list.
5	To assign data values to this value list.

4. If you typed **3**, the system displays the Copy Value List panel; continue to step 5. If you typed **5**, the system displays the Value List Authorization screen; go to step 6.

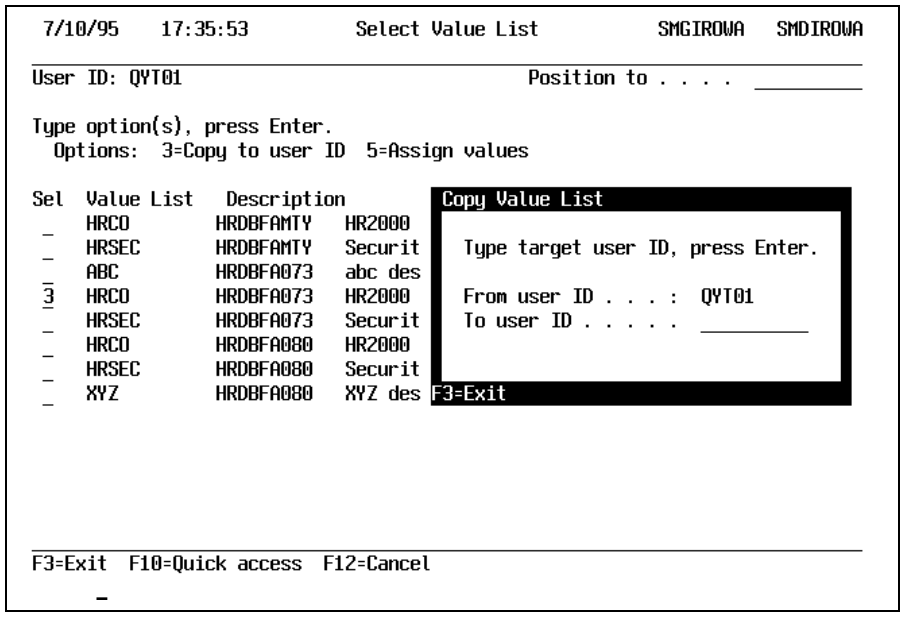


Figure 5-9: Copy Value List panel

5. The Select Value List panel lets you copy a value list associated with one user to apply that value list to one or more other users.

   Type the new user's ID and press Enter. The system performs the copying operation. Repeat for each additional user with whom you want to associate this value list.

   When done with this panel, press F3 to return to the Select Value List screen. Then go to step 6.

6. If you typed **5** in step 3, the system displays the Value List Authorization screen.

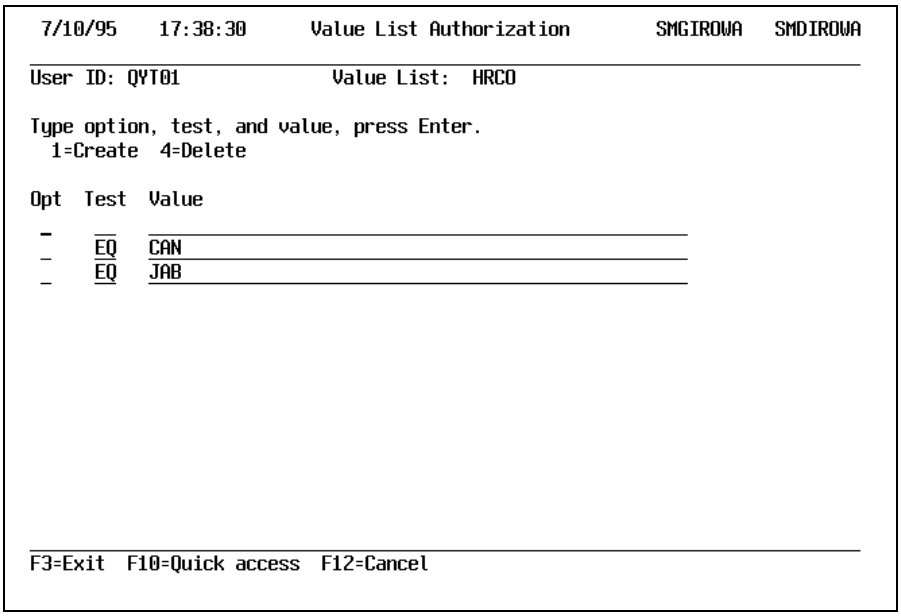


Figure 5-10: Value List Authorization screen

7. Perform any of the following tasks at this screen.

Task	Action
Delete an existing value list	Type **4** in the *Opt* column next to that list. At the deletion confirmation prompt, press Enter again to confirm the deletion, or F12 to cancel the deletion.
Create a new value list	Type **1** on the first data line in the *Opt* column. Type **EQ** (equals) or **NE** (does not equal) in the *Test* column. Type the values for the test in the *Value* column. Press Enter to complete entry of the new value list test. Examples: If this value list is defined in the *Definitions* menu as pointing to a company name field, and is being used to limit this user's access to records containing a company value of ABC, type **EQ ABC**. If this value list is to prevent the user from accessing records for company ABC, type **NE ABC**.
Edit an existing value list	Move the cursor to the appropriate line and edit the line.

When done with the Value List Authorization screen, press F3, type **1** at the Exit Options panel, and press Enter to save your changes and return to the Select Value List screen.

8. At the Select Value List screen, press F3 repeatedly to exit back to the Security *Authorizations* menu.