CA Datacom®

Security Reference Guide

Version 14.02

CA Technologies Product References

This document references the following CA products:

- CA Datacom®/DB
- CA Datacom® CICS Services
- CA Datacom® Datadictionary™
- CA Datacom® VSAM Transparency
- CA Dataquery™ for CA Datacom® (CA Dataquery)
- CA Ideal™ for CA Datacom® (CA Ideal)
- CA IPC
- CA Common Services for z/OS

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: CA Datacom Security Overview 11

Understanding Access Security 11
CA Datacom/DB Security 11
Plan Security 13
CA Datacom Datadictionary Security 13
CA Dataquery Security 14
SQL Security 14
- Table Security 14
- Plan Security 15
- View Security 15

External Security Product Publications 15
Disclaimer 15
Sample Report Headers 16
Reading Syntax Diagrams 17
Listing Libraries for CA Datacom Products 22

Chapter 2: Using External Security for CA Datacom 23

Considerations 23
- Prerequisites 24
- Security Audits and Reporting 24
- Access Validation 24

Setting Up Resource Classes 24
- Process Overview 26
- Using the DTSYSTEM 27
- DTADMIN 32
- Table Classes 32
- DTUTIL 33

DBUTLTY and External Security 35
- DBUTLTY Resource List 36

CA Datacom Datadictionary and External Security 42
- Internal Overrides 42
- DTADMIN Resource Class 43
- DTUTIL Resource Class 43
- Replication of Internal CA Datacom Datadictionary Security Levels 51
- Profiles 54

CA Dataquery and External Security 57

Internal Overrides 58
CA Dataquery Resource List 58
Table Authorizations 60
PDB and STORE Considerations 60
CA Dataquery Batch Utility Functions 61
Enabling Online Signons 61
Sample CA Command Resource Definitions 65
Security Interfaces, CA-ACF2 (z/OS and z/VSE) 66
Defining Resources 66
Defining Users 68
Defining Access Rights of a User 68
Defining Access Rights to Tables 69
Securing the MUF (DTSYSTEM) 72
Activating External Security 73
Path Security 74
Security Interfaces, CA Top Secret (z/OS) 75
Adding a Facility 76
Sample Entries to Secure CA Datacom 78
Defining Access Rights of Users 78
Security Interfaces, CA Top Secret (z/VSE) 78
Adding a Facility 79
Defining Access Rights of Users 81
Security Interfaces, RACF 81
Refreshing RACF Without Cycling Multi-User 83

Chapter 3: DD Internal Security 87

Securing CA Datacom Datadictionary Resources 87
CA Datacom Datadictionary Security Features 88
Security Level 89
Online Panels 89
Batch Transactions 89
Profiles 89
CA Datacom Datadictionary Security Model 90
Security Level (SRT) 90
Profiles 91
Facilities 92
Entity-Types (TABLES) 93
Status 94
Function 94
Relationships 100
CA Datacom Datadictionary Security Authorization Process 101

Person Authorization 101
Profile Authorization 101
Facility Authorization 102
Entity Authorization 102
Status Authorization 102
Function Authorization 103
Profiles Provided with CA Datacom Datadictionary Security 103
$DD-SEC-ADM Profile (Security Administrator) 103
Predefined Profiles 103
User-Defined Profiles Examples 105
Planning for CA Datacom Datadictionary Security 106
Determining Security Strategy 106
Identifying Resources and Personnel to Secure 106
Implications of CA Datacom Datadictionary Security 107
Implementing CA Datacom Datadictionary Security 109
Installing CA Datacom Datadictionary Security 110
Using CA Datacom Datadictionary Online Security Maintenance 111
Types of Panels 112
Menu Panels 114
Prompter Panels 114
Display Panels 115
Updating CA Datacom Datadictionary 117
Using PF and PA Keys 118
Using Command Processing 119
Using Line Commands 137
Using the Online Work Queue 138
Profile Maintenance Panel Error Codes 140
Signing On to CA Datacom Datadictionary Online 141
Adding CA Datacom Datadictionary Profiles 142
Cataloging Profiles 147
Deleting Profiles 149
Displaying Index of Profiles 150
Displaying Person Definitions 152
Displaying Profile Definitions 155
Displaying Profile Usage 157
Maintaining Persons 159
Updating Profiles 163
Updating Profile Entity-Types 169
CA Datacom Datadictionary Batch Security Maintenance 172
Maintaining and Cataloging Profiles 172
Header Transactions 173
-ADD and -UPD Transactions 173

Maintaining Persons 178
Producing a Security Report 180

Chapter 4: DQ Internal Security 187

Understanding CA Dataquery Security Concepts 187
Securing CA Dataquery Access Through Signon Procedures 189
Securing Data Access Through User Authorization 189
Securing Access to Tables, Rows, Columns, and Queries 190
Adding Users 191
CA Dataquery and External Security 191
Authorizing Users in CA Dataquery 192
CA Dataquery and External Security 195
Internal Overrides 195
Accessing User Information 196
Adding a New User 197
Updating a User 206
Managing Active Users 207
Deleting a User 210
Authorizing Administrative Functions 212
Limiting User Functions to Manipulate Data 215
Adding and Changing Passwords 215
Assigning Passwords to Users and to Groups 216
Assigning Group Levels 216
Assigning a Password to a User 217
Assigning a Password to a Group or a System 218
Deleting Passwords 221
Performing User Table Maintenance (DQUSERMT) 222
User Table Maintenance Control Statements 222
SIGN/ON Statements 223
ADD and UPDATE Statements 224
ADD and UPDATE Statement Optional Keywords 225
JCL Examples 234
DELETE Statement 235
REPORT Statement 235
Securing Data Access for DQL Use 236
Limiting Access to Database Tables 237
Authorizing Data Access Using the Security Maintenance Menu 238
Specifying Table Options Using the USER Option 240
Naming a CA Datacom/DB Database and Table for User Access 248
Limiting Access to Columns 253
How to Limit Access to Columns 253

Authorizing Access to Protected Columns 255
Viewing and Modifying Profile Codes Related to One User 255
Adding Profile-Code Authorizations 256
Limiting Access to Rows Using Conditions and Restrictions 257
Maintaining Conditions 258
Creating or Modifying a Restriction 265
Sample Condition and Restriction 269
Condition/Restriction Reporting (DQCRRPT) 272
Securing Data Access for SQL Use 278
Assigning Password Access 279
Limiting SQL Authorization 279
Limiting Access to Queries 280
Using Schemas 280
Creating Personal Tables 281
Assigning Access to Portions of Tables 282
Using SYNONYM Access 282
Considering CA Datacom System Security 283

Chapter 5: CA Datacom SQL Security 285

SQL Security Model 285
Resource Control 285
Access Rights 286
Naming Accessor IDs in GRANT and REVOKE 287
Validation Process 287
Activating and Maintaining 287
Implementing the SQL Security Model 288
Creating SQL Authorizations 288
Table-Level and View-Level Authorizations 289
View Security 289
Adding View Security Authorizations 291
Synonyms 297
Column-Level Authorizations 298
Plan Authorizations 298
Authorization for PUBLIC Access 298
CATALOG Authorization 298
Global Ownership 299
Deleting Access Rights 299
Cascading of REVOKE and DROP 299
Binding of GRANT and REVOKE Statements 300
Required Access Rights 300
SQL Statements and SQL Security Access Rights 300

CA Datacom/DB Commands and SQL Security Access Rights 306
Plan Security 308
Controlling Access to Plans 309
Plan EXECUTE and Plan BIND Privileges 310
Plan Options in Plan Security 312
CHECKBINDER System Privilege 314

Chapter 1: CA Datacom Security Overview

Understanding Access Security

Access security is the part of a security plan that controls access to data and functions. Without access security, individual user authorizations are not validated. Therefore, any user who can communicate with the Multi-User Facility (MUF) can obtain and modify data. CA Datacom security allows you to control access by providing security models.

With CA Datacom Datadictionary internal security and CA Dataquery internal security, each product is protected by access rules defined and maintained within that product. To protect CA Datacom Datadictionary and CA Dataquery with internal security, learn the security systems associated with each product.

External security provides the ability to control and administer user access to CA Datacom products and data based on the security profiles that exist in the external security product, such as CA ACF2, CA Top Secret, or RACF (z/OS).

The difference between external and internal security is where the user access authorizations are maintained.

CA Datacom/DB Security

CA Datacom/DB security protects access to tables and the CA Datacom/DB Utility (DBUTLTY) functions. This security is typically administered through an external security product.

Security User IDs

CA Datacom/DB is called by user applications. As part of shipping a request to the MUF, the current user ID is passed. In the MUF, this user ID is signed on with a technique not requiring a password. This technique requires that the MUF be authorized. The MUF does *not* enable if external security is established for the Directory and the MUF is not authorized.

The MUF maintains the signed on users in an unlimited cache that contains both the signon and tables that have been accessed successfully in the past. As each request is made, it is validated by first checking the cache. If it is found, no further checks are needed. If it is not found, external security is called.

Because CA Datacom/DB saves authorizations in memory, it is not always in synchronization with the external security product. For most products (except notably RACF), when it is necessary for a change to be seen instantly, use the DBUTLTY SECURITY OPTION=RESET transaction or the console command SECURITY RESET to reset the security buffer. You can specify either an individual user be reset or all users be reset. If you specify a user on the reset, the MUF signs that individual user off and all of the cached permissions of that user are discarded. If you do not specify a user, the MUF signs all users off, and the entire cache is discarded, which in turn causes reestablishment of all security validations.

When updating RACF resources, The RACF environment is *not* automatically refreshed. However, there is a method that allows the RAC LIST to be refreshed without recycling the MUF. For more information, see Refreshing RACF Without Cycling Multi-User (see page 83).

Note: The security user ID is part of the log record and is reported with the RXX report. The security user ID is also part of the READRXX fields.

Security and User Exits

CA Datacom/DB has three user exists and the MUF allows a subtask. These facilities allow code other than CA Datacom/DB to open data sets and perform work. When reviewing your security environment and setting up external security, review these programs (if any) and verify that you are not allowing access to secured data by user programs hidden in the MUF region.

SQL Security Supersedes

If the SQL Security Model is defined for a database, only privileges defined with GRANT and REVOKE statements are used to control access to the tables in that database. In this case, these security authorizations supersede any external authorizations.

Table Partitioning Considerations

If a DBUTLTY function does not include an explicit TABLE= keyword, table level security (at the DBUTLTY) can be granted either at the Full Parent table level or the Child table level. If the DBUTLTY function includes a specific TABLE= keyword, table level access is checked using the table name specified by the TABLE= keyword. For example, the EXTRACT function of DBUTLTY uses the table name specified in the TABLE= keyword. But a DBUTLTY BACKUP AREA function uses either the Childrens' names that are contained in the area, or it uses the Full Parents table names. If access is granted to either, the BACKUP is allowed.

Plan Security

Plan security allows you to give explicit rights to an SQL plan. When you give explicit rights to an SQL plan, that plan and its associated program can be executed without specific access rights to the tables or views accessed by that plan. However, any non-SQL statement executed from the same program is checked according to the security profile for the tables accessed by the native command.

You can administer SQL plan security by using SQL GRANT and REVOKE statements that use SQL security for table and views as discussed under Table Security.

SQL plan security can also be administered by using external security facilities. SQL plan security can therefore be combined with the external table security model to provide a single-source security model. We recommend that you administer plan security through external security.

CA Datacom Datadictionary Security

CA Datacom Datadictionary security protects product functions unique to the product. These functions include basic CA Datacom Datadictionary online (DDOL) and batch utility activities and entity-type function combinations. CA Datacom Datadictionary internal security supports its own signon. External security uses the external security accessor identification to validate the user and uses the externally defined authorizations to protect the CA Datacom Datadictionary functions.

The Security Administrator controls whether CA Datacom Datadictionary is secured with external security. If external security is selected for CA Datacom Datadictionary, then CA Datacom Datadictionary internal security authorizations are ignored. No modifications are required to CA Datacom Datadictionary to implement external security.

Note: CA Datacom Datadictionary internal security can be used even though CA Datacom/DB is using external security.

CA Dataquery Security

CA Dataquery security protects product functions unique to the product. These functions include CA Dataquery online and batch activity. CA Dataquery internal security uses a secondary product signon for each accessor and permits you to define Table Authorizations in CA Dataquery security. External security uses the external security user identification and validates table access according to the authorizations defined in CA Datacom/DB security.

The Security Administrator controls whether CA Dataquery is secured with external security. If external security is selected for CA Dataquery, then CA Dataquery internal security authorizations are ignored. No modifications are required to CA Dataquery to implement external security. Security settings for databases with DBIDs greater than 999 is only supported in external security.

Using the CA Datacom/DB SECURITY Multi-User startup option and your external security product, CA Dataquery security is recognized as a separate path in CA Datacom/DB with the LEVEL05 PASS/FAIL resource. If the proper permissions are set for the level 05 resource, you can specify four paths specifically for CA Dataquery.

Note: CA Dataquery internal security can be used even though CA Datacom/DB is using external security.

SQL Security

SQL security includes table, plan, and view security.

Table Security

An alternate way to protect table access is to use SQL GRANT and REVOKE statements. In this case, CA Datacom/DB security is still used to protect DBUTLTY functions and to control who can create tables and authorization IDs. You can use the ANSI-compliant SQL GRANT and REVOKE statements only to control access to tables and views.

You can choose to protect table access by CA Datacom/DB security or by SQL security at the database level by specifying YES or NO for the SQL-SECURITY attribute when defining databases to CA Datacom Datadictionary.

SQL table security cannot be administered externally.

Plan Security

Plan security allows you to give explicit rights to an SQL plan. When you give explicit rights to an SQL plan, that plan and its associated program can be executed without specific access rights to the tables or views accessed by that plan. However, any non-SQL statement executed from the same program is checked according to the security profile for the tables accessed by the native command.

You can administer SQL plan security by using SQL GRANT and REVOKE statements that use SQL security for table and views as discussed under Table Security.

SQL plan security can also be administered by using external security facilities. SQL plan security can therefore be combined with the external table security model to provide a single-source security model. We recommend that you administer plan security through external security.

View Security

Enabling views to secure by name gives greater control because it allows control of access to the precise set of tables, rows, and columns defined by a view. View security replaces security authorization checks on the individual tables referenced by a view with a check against the view entity itself. This allows the owner of the tables to restrict complete access to the tables but still permit a view of specific data to certain users. This feature is activated in the external security package.

External Security Product Publications

If your site uses an external security product, such as CA ACF2, CA Top Secret, or IBM RACF, you need the complete set of the documentation for that product.

Disclaimer

The sample code, JCL, and reports provided in this guide are intended for use as reference aids only. No warranty of any kind is made as to the completeness or correctness of the exact samples in your specific installation environment. If you are planning to use any of the samples provided in this guide, be sure to adjust them for your site standards and use.

Sample Report Headers

The report headers for the sample reports contained in this guide are shown here. Report headers have the following format:

```
Date: mm/dd/ccyy    ********************************************************************************         Page:     1
                    *                                CA Datacom/DB                                 *
Time: hh.mm.ss      *                              General Utility                                 *      Version: 14.0
                    *                Copyright © 1990-2011 CA. All rights reserved.                *
Base:     dbid      ******************************************************************************** Directory: name
```

Base:

The *dbid* is the DATACOM-ID (DBID) of the database (base) in use when the report was built.

Note: Base does not appear in the header if it is not appropriate for the report that was generated or not known at the time the report is produced.

Date:

The date when the report was executed is shown in the format *mm/dd/ccyy*:

mm

month

dd

day

cc

century

yy

year

Directory:

The *name* is the internal name of the Directory (CXX), assigned with the INIT CXX function, that was in use when the report was executed and if known at the time the report was produced.

Note: Directory does not appear in the header if it is not appropriate for the report that was generated.

Page:

The *n* is the page number of the report.

Time:

The time when the report was assembled is shown in the format *hh.mm.ss*:

hh

hour

mm

minutes

ss

seconds

Version:

The version of CA Datacom/DB being executed when the report was built is shown in the format *nn.n,* for example, Version: 14.0.

Reading Syntax Diagrams

Syntax diagrams are used to illustrate the format of statements and some basic language elements. Read syntax diagrams from left to right and top to bottom.

The following terminology, symbols, and concepts are used in syntax diagrams:

- Keywords appear in uppercase letters, for example, COMMAND or PARM. These words must be entered exactly as shown.
- Variables appear in italicized lowercase letters, for example, *variable*.
- Required keywords and variables appear on a main line.
- Optional keywords and variables appear below a main line.
- Default keywords and variables appear above a main line.
- Double arrowheads pointing to the right indicate the beginning of a statement.
- Double arrowheads pointing to each other indicate the end of a statement.
- Single arrowheads pointing to the right indicate a portion of a statement, or that the statement continues in another diagram.
- Punctuation marks or arithmetic symbols that are shown with a keyword or variable must be entered as part of the statement or command. Punctuation marks and arithmetic symbols can include the following:

,	comma	>	greater than symbol
.	period	<-	less than symbol
(	open parenthesis	=	equal sign

)	close parenthesis	¬	not sign
+	addition	-	subtraction
*	multiplication	/	division

The following is a diagram of a statement without parameters:

Statement Without Parameters

For this statement, write the following:

```
COMMAND
```

Required parameters appear on the same horizontal line, the main path of the diagram, as the command or statement. The parameters must be separated by one or more blanks.

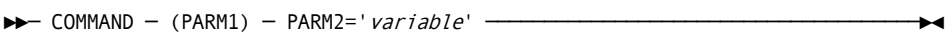
Statement with Required Parameters

Write the following:

```
COMMAND PARM1 PARM2
```

Delimiters, such as parentheses, around parameters or clauses must be included.

Delimiters Around Parameters

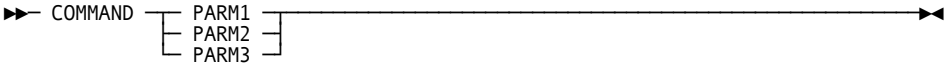


If the word *variable* is a valid entry, write the following:

```
COMMAND (PARM1) PARM2='variable'
```

When you see a vertical list of parameters as shown in the following example, you must choose one of the parameters. This indicates that one entry is required, and only one of the displayed parameters is allowed in the statement.

Choice of Required Parameters

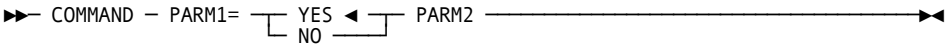


You can choose one of the parameters from the vertical list, such as in the following examples:

```
COMMAND PARM1
COMMAND PARM2
COMMAND PARM3
```

When a required parameter in a syntax diagram has a default value, the default value appears above the main line, and it indicates the value for the parameter if the command is not specified. If you specify the command, you must code the parameter and specify one of the displayed values.

Default Value for a Required Parameter

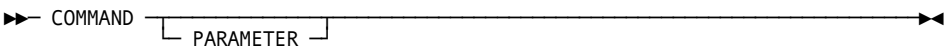


If you specify the command, you must write one of the following:

```
COMMAND PARM1=NO PARM2
COMMAND PARM1=YES PARM2
```

A single optional parameter appears below the horizontal line that marks the main path.

Optional Parameter

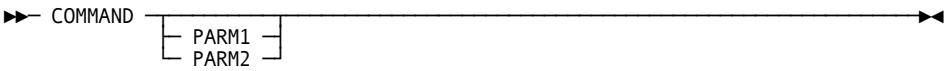


You can choose (or not) to use the optional parameter, as shown in the following examples:

```
COMMAND
COMMAND PARAMETER
```

If you have a choice of more than one optional parameter, the parameters appear in a vertical list below the main path.

Choice of Optional Parameters

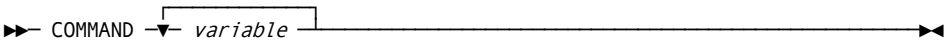


You can choose any of the parameters from the vertical list, or you can write the statement without an optional parameter, such as in the following examples:

```
COMMAND
COMMAND PARM1
COMMAND PARM2
```

In some statements, you can specify a single parameter more than once. A repeat symbol indicates that you can specify multiple parameters.

Repeatable Variable Parameter

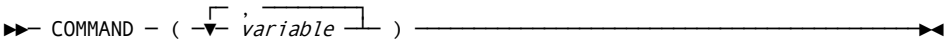


In the preceding diagram, the word *variable* is in lowercase italics, indicating that it is a value you supply, but it is also on the main path, which means that you are required to specify at least one entry. The repeat symbol indicates that you can specify a parameter more than once. Assume that you have three values named VALUEX, VALUEY, and VALUEZ for the variable. The following are some of the statements you can write:

```
COMMAND VALUEX
COMMAND VALUEX VALUEY
COMMAND VALUEX VALUEY VALUEZ
```

If the repeat symbol contains punctuation such as a comma, you must separate multiple parameters with the punctuation. The following diagram includes the repeat symbol, a comma, and parentheses:

Separator with Repeatable Variable and Delimiter

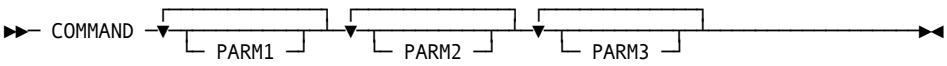


In the preceding diagram, the word *variable* is in lowercase italics, indicating that it is a value you supply. It is also on the main path, which means that you must specify at least one entry. The repeat symbol indicates that you can specify more than one variable and that you must separate the entries with commas. The parentheses indicate that the group of entries must be enclosed within parentheses. Assume that you have three values named VALUEA, VALUEB, and VALUEC for the variable. The following are some of the statements you can write:

```
COMMAND (VALUEC)
COMMAND (VALUEB,VALUEC)
COMMAND (VALUEB,VALUEA)
COMMAND (VALUEA,VALUEB,VALUEC)
```

The following diagram shows a list of parameters with the repeat symbol:

Optional Repeatable Parameters

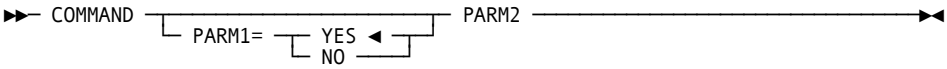


The following are some of the statements you can write:

```
COMMAND PARM1
COMMAND PARM1 PARM2 PARM3
COMMAND PARM1 PARM1 PARM3
```

The placement of YES in the following diagram indicates that it is the default value for the parameter. If you do not include the parameter when you write the statement, the result is the same as if you had specified the parameter with the default value.

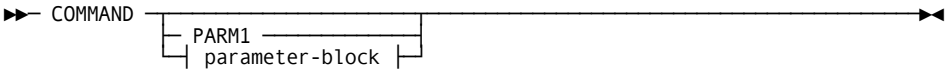
Default Value for a Parameter



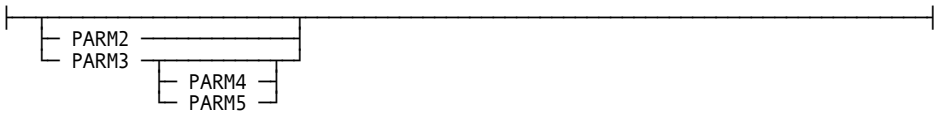
For this command, COMMAND PARM2 is the equivalent of COMMAND PARM1=YES PARM2.

In some syntax diagrams, a set of several parameters is represented by a single reference.

Variables Representing Several Parameters



Expansion of parameter-block



The *parameter-block* can be displayed in a separate syntax diagram.

Choices you can make from this syntax diagram therefore include, but are not limited to, the following:

```
COMMAND PARM1
COMMAND PARM3
COMMAND PARM3 PARM4
```

Note: Before you can specify PARM4 or PARM5 in this command, you must specify PARM3.

Listing Libraries for CA Datacom Products

Guidelines to assist you in preparing your JCL are provided in this guide. The sample code provided in this document is intended for use as a reference aid only and no warranty of any kind is made as to completeness or correctness for your specific installation.

Samples for JCL and programs are provided in the install library (in z/OS, the default name for this library is CABDMAC). In z/VSE, sample PROCs are provided that allow you to use parameter substitution. You can copy and modify these samples for your specific requirements.

Code JOB statements to your site standards and specifications. Specify all data set names and library names with the correct names for the installation at your site. In many examples, a REGION= or SIZE= parameter is displayed in an EXEC statement. The value displayed should be adequate in most instances, but you can adjust the value to your specific needs.

The libraries listed for searching must include the following in the order shown:

1. User libraries (*hlq*.CUSLIB) you may have defined for specially assembled and linked tables, such as DBMSTLST, DBSIDPR, DDSRTLM, DQSYSTBL, or User Requirements Tables
2. CA Datacom base libraries (*hlq*.CABDLOAD): CA Datacom/DB, CA Datacom Datadictionary, CA Dataquery
3. CA Common Services for z/OS base libraries (*hlq*.CAW0LOAD)
4. CA IPC libraries (*hlq*.CAVQLOAD)
5. Libraries for additional products, such as [assign the DCS variable value for your book], CA Datacom VSAM Transparency, CA Ideal, and so on

Chapter 2: Using External Security for CA Datacom

External CA Datacom security provides users the option of defining CA Datacom product resources, accessors, and access rules using one external security package. This organization standardizes security across products, simplifies security administration, and allows the Security Administrator to control security without becoming an expert on the products being secured.

The method used to associate CA Datacom product resources with users is specific to the external security package used. Consult your security product documentation for complete details.

Considerations

To externalize CA Datacom security, decisions about user access to product functions and data must be made and relayed to the Security Administrator. In turn, the Security Administrator conveys the information to the external security product by constructing resources to represent each access right or level. Each resource directly controls access to a specific function in a CA Datacom product.

Externally securing all CA Datacom products can be a major undertaking. It is important that the product administrators, who can provide product-specific information, participate in the task of securing their products.

Once CA Datacom resources are stored in the external security product and the appropriate initiation steps taken, the external security product has control. CA Datacom products defer to external security with the exception of SQL security.

The following are discussed in this overview of using external security for CA Datacom/DB:

- Prerequisites
- Security Audits and Reporting
- Access Validation

Prerequisites

CAIRIM and the CA IPC are required for external security. You installed these before installing CA Datacom products.

Note: CAIRIM is part of CA Common Services for z/OS and part of CA CIS for z/VSE (formerly known as CA90s Services).

The CA Standard Security Facility (CAISSF), a subcomponent of CAIRIM, provides the link between the CA Datacom products and the external security product. The CAISSF is a prerequisite for implementing external security.

The CA IPC is required for CA Datacom Datadictionary and CA Ideal online signon.

Note: For more information, see the *CA IPC Implementation Guide* and Enabling Online Signons (see page 61).

Security Audits and Reporting

When external security is in effect, the external security product controls audits and reporting.

Access Validation

Once it has identified the user, the Security Facility determines if the resource is in a database secured under the SQL Security Model or the CA Datacom/DB Security Model. The Security Facility then validates the rights of the user based on the rules or permissions in the external security package or SQL security.

Setting Up Resource Classes

This section provides information about resource class names and formats for securing the CA Datacom products in CA ACF2, CA Top Secret, or IBM's RACF.

CA Datacom products share the following CA Datacom resource classes in the external security products. The external security product controls the user access rights and levels. The method used to tie the user to functions or data depends on the security product used.

Resource Class Names

The resource class names used in this chapter represent generic names. Your specific external security product may use slightly different resource class, or resource type, names.

- For CA ACF2, see Security Interfaces, CA-ACF2 (z/OS and z/VSE) (see page 66).
- For CA Top Secret, see Security Interfaces, CA Top Secret (z/OS).
- For IBM RACF, see Security Interfaces, RACF (see page 81).

Type of Information	Resource Class	Products Using	Access Levels
System	DTSYSTEM	CA Datacom/DB CA Datacom Datadictionary CA Dataquery CA Datacom/DB SQL Option	None
Administrator	DTADMIN	CA Datacom/DB CA Datacom Datadictionary CA Datacom/DB SQL Option	None
Table	DTTABLE DCTABLE DFTABLE DGTABLE DHTABLE DPTABLE DQTABLE DRTABLE DSTABLE DXTABLE	CA Datacom/DB CA Datacom/DB SQL Option CA Dataquery	READ ADD UPDATE DELETE
Utility	DTUTIL	CA Datacom/DB CA Datacom Datadictionary CA Dataquery CA Datacom/DB SQL Option	None

The following apply to conventions used for CA Datacom and in this chapter:

- Resource names contain no embedded blanks.
- Uppercase values are constants in the resource name.

- Lowercase values indicate variables.
- The system identifier is the CA Datacom/DB Directory (CXX) name unique to each system. If two or more MUFs share the same Directory, they share the same CXX name.
- DDutility and DQutility represent a number of possible product programs or functions.

Some external security products allow you to use prefixing, masking, and patterning techniques. These can include fixed position character substitution, or wildcards, and variable character substitution, or masking, when defining resources. Some products also allow you to define profiles and then assign users to specific profiles for permissions. These techniques allow you to reduce the number of resource definitions. See your external security product documentation for the availability and use of these features.

Process Overview

When you enable the MUF, external security is called to determine the security status. The first determination made is the level of security that you are running. When CA Datacom implements new security features, it does so by implementing a new level of security in the DTSYSTEM resource class. The current highest level of support is LEVEL05. All other levels, that is levels 01 through 04, are still supported, but we recommend that you implement security at the highest supported level, that is, LEVEL05. Each higher level supports all the features contained in lower levels and new features.

A level consists of a pair of resource names in the DTSYSTEM resource class. The resource names are ACTIVATE.LEVELnn.PASS and ACTIVATE.LEVELnn.FAIL. A check is made at Multi-User startup for LEVEL05 using the user ID associated with the MUF. If access is allowed to the PASS resource and access is denied for the FAIL resource, the level is considered in force and further checks are made based on the level. If either of these is not true, CA Datacom/DB checks the PASS/FAIL resources at the next level, in this case level 04, until it either finds the correct combination or it exhausts all the levels.

All the following documentation pertains to the complete set of features available at level 05. Following is a list of features that are available at lower levels.

Level 04

Is the same as level 05, except CA Dataquery path security is not checked for or allowed.

Level 03

Is the same as level 04, except that view security is not checked for or allowed.

Level 02

Is the same as level 03, except that the number of paths recognized is two:

- SQL (for all SQL requests)
- RAT (for all non-SQL requests)

Only two table classes are available at this level: DTTABLE and DXTABLE.

Level 01

Is the same as level 02 except all paths are treated equally using DTTABLE for table access. External security for all of CA Datacom/DB is enabled by denying permission to DTSYSTEM resource cxxname.DB.

Note: XCF cannot be externally secured at level 01.

Before the appropriate level permissions are set, it is important that all desired information is stored in the other resource classes. That is, review the DTADMIN, the DCTABLE and DTUTIL classes and add required entries before securing the Directory with the DTSYSTEM resource.

Using the DTSYSTEM

In addition to being used for level checking, the DTSYSTEM class identifies the following:

- Whether certain features are externally securable,
- Whether CA Datacom Datadictionary or CA Dataquery are externally secured, and
- Which table classes can be used to secure table access for various access paths.

Note: Security event logging to the console is normally suppressed on DTSYSTEM resource calls made during Multi-User startup.

Each of the non-level DTSYSTEM resource names begin with a high-level node of CXX name that identifies a system. A system includes all the databases and tables defined in the CA Datacom/DB Directory (CXX) represented by the CXX name. The CXX name is established for a CXX when the CXX is initialized.

The DTSYSTEM resource class is the key to turning on external security for CA Datacom products. To activate external security, the Security Administrator must deny all users access to the DTSYSTEM resource which identifies the system to secure. To deactivate external security, the Security Administrator must allow all users access to the DTSYSTEM resource identifying the unsecured system. The CXX name identifies the system.

At the startup of the MUF, when the LEVEL PASS and FAIL resource names are properly set up, the external security product is called with a series of resource names in the DTSYSTEM resource class. These resource names have a high-level node of the cxxname followed by a low-level node or nodes representing a product or feature. The following list shows what these resource names represent and what it means if the user who submitted the MUF is denied access to these resource names.

Note: Each of the following products or features, when externally secured, produces a DB00220I message to indicate that it is externally secured.

cxxname.DQ

CA Dataquery is externally secured

cxxname.DD.

CA Datacom Datadictionary is externally secured.

cxxname.XCF

XCF is externally secured.

Note: The check for XCF security is only done for those operating system environments that support XCF.

cxxname.SV.ENABLE

View security allowed.

cxxname.SV.DEFAULT

Default view security may be specified on the Multi-User startup options.

The DTSYSTEM resource class also allows the Security Administrator to define the security mode for any new Multi-User system not yet defined. If the default permission is allowed for undefined systems, new systems are not secured. When the default permission is denied and LEVEL03 or higher is properly set (such as in CA ACF2), new systems are protected and permissions must be in place for all CA Datacom/DB activities before the CA Datacom/DB Directory initialization. If LEVEL03 or higher has been properly set, "default deny" allows the Database Administrator to choose the level of external security for undefined MUF.

If you have defined LEVEL03 or higher resource name pairs, coded path definitions in the Multi-User startup option SECURITY, and if the path-class access is denied, access to this particular path-class is secured.

Other Products Use of DTSYSTEM

If any level is selected, cxxname.DD and cxxname.DQ are also checked. If access is denied for cxxname.DQ, CA Dataquery is externally secured.

If LEVEL03 or higher external security is in place (through DTSYSTEM resources) and the operating system environment is such that XCF could run against this MUF, an additional security check is done using the DTSYSTEM resource class and a resource name of cxxname.XCF. If permission is denied to the user who submitted the Multi-User, XCF external security is in place.

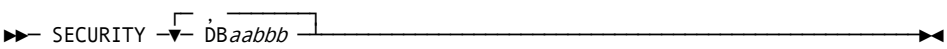
Beginning with 14.0, the XCF_FROM specifications have become more dynamic and flexible. Therefore, if XCF is externally secured, each remote job which uses XCF to connect to MUF has its security checked at open or connection time.

This check is made against the DTSYSTEM resource class using a resource name of cxxname.XCFFROM.from-system.groupname (corresponding to the system from which the job is connecting and the XCF group it is using to connect). This check is done using the user who submitted Multi-User. If the check is denied, the open fails with a return code 87 (003) and no connection is established by the job.

SECURITY Multi-User Startup Option

Path security allows you to identify security rules for different command paths.

SECURITY (Path Security Syntax)



DB*aabbb*

(Required) This is the format of a path security class-and-path option parameter, where *DB* is a constant.

The *aa* in the format represents valid class codes. These class codes correspond to the table classes defined in the external security system. Those table classes must be defined **before** implementing path security in CA Datacom/DB.

The valid entries and the table classes to which each corresponds are:

DC

Corresponds to DCTABLE

DF

Corresponds to DFTABLE

DG

Corresponds to DGTABLE

DH

Corresponds to DHTABLE

DP

Corresponds to DPTABLE

DQ

Corresponds to DQTABLE

DR

Corresponds to DRTABLE

DS

Corresponds to DSTABLE

DT

Corresponds to DTTABLE

DX

Corresponds to DXTABLE

NO

Specifies no path security for the indicated path (bbb)

The *bbb* in the format represents one of the valid path codes you can secure with path security. By specifying multiple class-and-path options, you can, if needed, specify in any order all ten different path codes on multiple lines as long as all paths specified are unique. But each separate path code can only be used once per SECURITY Multi-User startup option. When you specify multiple class-and-path options, you must use a comma to separate each occurrence, as indicated in the syntax diagram and shown in the following example.

The valid path code entries and what they signify are:

SCI

CICS SQL requests path

SCQ

CICS SQL for CA Dataquery requests path

RCI

CICS non-SQL requests path

RCQ

CICS non-SQL for CA Dataquery requests path

RAQ

Non-CICS non-SQL for CA Dataquery requests path

SSR

CA Datacom Server or Ingres Enterprise Access to CA Datacom SQL requests path

RSR

CA Datacom Server or Ingres Enterprise Access to CA Datacom non-SQL requests path

SQL

Non-CICS, non-CA Datacom Server, and non-Ingres Enterprise Access to CA Datacom SQL requests path

SQQ

SQL non-CICS for CA Dataquery requests path

RAT

All other non-SQL paths

Example

The following is an example showing the use of six path code options in one SECURITY Multi-User startup option. Path codes can be listed in any order, that is, the order shown in this example is only one of many possible orders.

```
SECURITY DBaaSSR,DBaaRAT,DBaaSCI,DBaaRSR,DBaaSQL,DBaaRCI
```

Note: There is no restriction on how many times a class code can be used per SECURITY Multi-User startup option. You could, for example, use the same class code for the different path code occurrences.

An example of a Multi-User startup option with six possible path-and-class options is:

```
SECURITY DBDTRAT,DBDCSCI,DBDRSSR,DBDFRCI,DBDSSQL,DBDXRSR
```

If a path-and-class is specified in the Multi-User startup option, a security check is issued for the DTSYSTEM class with a resource name cxxname.path-and-class. The path-and-class name must exactly match the seven letters coded in the Multi-User startup option. If access is denied, this path is secured using the class specified. If access is granted, an error is returned and the Multi-User is not enabled.

Any paths not coded in the Multi-User startup option have all possibilities checked for the path, that is, the ten classes and NO using DTSYSTEM resource class and names of cxxname.path-and-class. If access is denied to more than one of the options for this path, an error is returned and the Multi-User does not enable. If access is allowed for all options, no security is in place for this path.

DTADMIN

The DTADMIN class associates system product combinations with those individuals who have product administrator authority. Product privileges derived from administrator authority vary by product. The DTADMIN resource name consists of the CXX name plus the two-character product code (DB or DD). It is associated with a user accessor ID (ACID).

A user who has access to the DTADMIN resource cxxname.DB is considered a Global Owner and can perform the following:

- Create a schema for SQL.
- Issue the GRANT and REVOKE commands for any SQL controlled table.
- Issue the DROP command any table.

A user who has access to the DTADMIN resource cxxname.DD is considered a CA Datacom Datadictionary Security Administrator and can perform the following:

- Run the batch 4099 Field Access transaction.
- Add and maintain relationship definitions.

Table Classes

The table classes identify CA Datacom/DB tables and multiple access levels for each table. The valid table classes are:

- DCTABLE
- DFTABLE
- DGTABLE
- DHTABLE
- DPTABLE
- DQTABLE
- DRTABLE
- DSTABLE
- DTTABLE
- DXTABLE

The MUF recognizes ten possible access paths. Ten table classes therefore exist. Because each class has no intrinsic meaning, you can mix and match which classes are used for which paths, using each of the ten table classes for each unique path or assigning multiple paths to the same class. The SECURITY Multi-User startup option combined with the resource names defined to the DTSYSTEM resource class determines which class to use for which paths. The external security product handles the task of tying users to tables and access levels. The access levels correspond to the following CA Datacom/DB access rights:

- ADD
- DELETE
- READ
- UPDATE

Note: CA Top Secret z/OS allows READ access if UPDATE access is specified. RACF treats access levels in a hierarchical way. For more information, see Security Interfaces, RACF (see page 81).

The table class resources consist of system, database, and table identifiers in the following format:

```
cxxname.DB0nnnn.table
```

For example, DBMUF001.DB00140.PAY identifies the PAY table in the database with DBID 140 in the system DBMUF001.

DTUTIL

DBUTLTY is secured using the DTUTIL resource class if any non-SQL access path is secured. For example, record-at-a-time commands. Most CA Datacom/DB Utility (DBUTLTY) functions secure table access through a DTUTIL resource. A few functions secure READ or ADD access using the specified table class for the record-at-a-time path.

The DTUTIL resource class is used to identify CA Datacom product utility functions and the users that are allowed to execute them. Each resource in the DTUTIL class represents one CA Datacom product function. The resource format varies within and for each of the three products it supports.

The following are the formats that are discussed later in this chapter:

```
cxxname.DBUTLTY.function.subfunction
cxxname.DB0nnnn.table.right
cxxname.DQutility.function
cxxname.DD0nnnn.DDutility.function
cxxname.DD0nnnn.table.status.function
cxxname.SQCHECKBINDER
cxxname.SQEXE.plan-authid.plan-name
cxxname.SQBND.plan-authid.plan-name
```

Some DTUTIL resource class security calls are done using LOG=NONE. They are internal CA Datacom product calls that need to be performed when a selected function spans multiple database resources but the user only has access rights to some of the resources. The resources to which the user does not have access are bypassed.

Externalization of Plan Security

The DTUTIL resource class can be used to secure the use of SQL plans.

Users of CA ACF2, CA Top Secret, and RACF can take advantage of SQL plan security by using statements in the security package. These statements are equivalent to the SQL GRANT and REVOKE statements to control the plan EXECUTE, plan BIND, and system level CHECKBINDER privileges.

Use the following resource names to secure plans. The resource class for all three resource names is DTUTIL. System-level authority to secure plans is established with cxxname.SQCHECKBINDER.

To execute and bind privileges on a plan:

```
cxxname.SQCHECKBINDER
cxxname.SQEXE.plan-authid.plan-name
cxxname.SQBND.plan-authid.plan-name
```

Because resource names are limited to 40 characters in at least one external security package, the combination of plan-authid, plan-name, and the "." should (assuming a cxxname of 8 characters) be limited to a maximum of 25 characters. This could be accomplished by establishing a naming convention limiting plan names to 16 characters and authids to 8 characters.

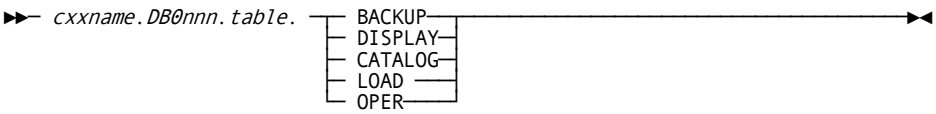
DBUTLTY and External Security

CA Datacom/DB uses all four resource classes for external security. The DTUTIL resource class is the only one with portions of the resource name defined by functions in the CA Datacom product. This section provides a list of valid resource names and a sample resource. (The CA Datacom/DB operator console commands are *not* secured by external security.)

Note: The DBUTLTY function COMM OPTION=CONSOLE, only requires rights to COMM.CONSOLE. If you are allowed these rights, you can perform any function the CONSOLE API supports. For more information, see the *CA Datacom/DB DBUTLTY Reference Guide*.

Certain DBUTLTY functions and subfunctions require access at the database and table level. The EXTRACT, MASSADD, and REPORT IXXDUMP functions require the database READ or ADD rights and these functions use the table class specified for the record-at-a-time path. All other functions are validated using the DTUTIL resource class. The format includes the database ID and table name followed by the access rights. AUTO functions also use the table class specified for the record-at-a-time path.

Resource Classes Used by CA Datacom/DB



A special case exists for the cxxname.DB0nnnn.table.CATALOG resource. The resource is used in the normal context, but also has a special use when creating a table through SQL. An SQL CREATE requires the CATALOG right to the database to contain the new table. This database right is done using the literal 999 instead of a table name.

DBUTLTY Resource List

DBUTLTY table access is secured mostly through DTUTIL. A few individual DBUTLTY functions can secure table access using resource class defined for non-SQL, non-Server, and non-CICS. These are DBUTLTY functions which require READ or ADD access at the table level.

The following is a list of valid CA Datacom/DB DTUTIL resources. Replace cxxname with a valid Directory (CXX) name. A resource format that includes tables applies to a function or subfunction that involves a database or area and can affect more than one table. In most cases, you must identify to the external security product each table that you want to allow or deny access.

- The COMM ERROR and REPORT IXXDUMP functions are for internal use only. Secure these functions for execution by the Database Administrator and execute only as directed by CA Support.
- The COMM EOJFREE, COMM EOJKEEP, COMM SNAPCSA, COMM SNAPSVC, and REPORT MEMORY functions are for z/OS systems only.
- The EDIT function of the CA Datacom/DB Utility (DBUTLTY) is not secured.
- The following syntax secures the corresponding DBUTLTY CXXMAINT options:

Keyword	CXXMAINT Option
ALTERDSN	ALTER DSN
ALTERDBC	ALTER DBCS
ALTERDSO	ALTER DSOP
ALTERKEY	ALTER CBSUSE KEYNAME
ALTERLNG	ALTER LANGUAGE
ALTERLNK	ALTER LINK
ALTERLOG	ALTER LOGGING
ALTEROP2	ALTER OPTION2
ALTERSIN	ALTER SINGLE (Single User)

- LOAD CXXBASE secures a specific DBID with the LOAD AREA=CXX option.
- SPILLREW is for z/VSE systems only.
- TESTDATA is used at installation to load the DEMO database.

The following is a list of valid CA Datacom/DB DTUTIL resources. The format of the DTUTIL resource name for the function is:

```
cxxname.DBUTLTY.function.subfunction
```

For most DBUTLTY functions, although some have no sub-function, in which case the format is:

```
cxxname.DBUTLTY.function
```

For DBUTLTY functions that include table access, the format of the DTUTIL resource name for table-level checks is:

```
cxxname.DB0nnnn.table.right.
```

Valid DTUTIL Resources

DTUTIL Function and Sub Function	DTUTIL Table Right	DnTABLE Access Level	Table	Tables
ACCESS	OPER			X
ACCT.CATALOG	OPER			X (includes PRM)
ACCT.CLOSE				
ACCT.EDIT	CATALOG			X (includes PRM)
ACCT.OPEN				
ACCT.SPILL				
AUTO*				
BACKUP.CXX				
BACKUP.DATA	BACKUP			X
COMM.ALTER				
COMM.CANCEL				
COMM.CLOSE				
COMM.CLRCBS				
COMM.CLRDST				
COMM.CLRPXX				
COMM.CLRML				

DTUTIL Function and Sub Function	DTUTIL Table Right	DnTABLE Access Level	Table	Tables
COMM.CLRSQL				
COMM.CONSOLE				
COMM.EOJ				
COMM.EOJFREE				
COMM.EOJKEEP				
COMM.NEWRXX				
COMM.REQABORT				
COMM.SNAP				
COMM.SNAPCSA				
COMM.SNAPSVC				
COMM.STATS				
COMM.STATUS				
CONFIRM				
CXXCLONE (if no DBID is specified, refer to the LOAD.CXX row, or if a DBID is specified, refer to the LOAD.CXXBASE row)				
CXXMAINT.ALTERDBC				
CXXMAINT.ALTERDSN	CATALOG			X
CXXMAINT.ALTERDSO	CATALOG			X
CXXMAINT.ALTERKEY	CATALOG		X	
CXXMAINT.ALTERLNG				
CXXMAINT.ALTERLNK	CATALOG			X
CXXMAINT.ALTERLOG	CATALOG		X	
CXXMAINT.ALTEROP2				
CXXMAINT.ALTERSIN				
CXXMAINT.CONVERT				
CXXMAINT.DDPROD	CATALOG			X
CXXMAINT.DELETE	CATALOG		X	

DTUTIL Function and Sub Function	DTUTIL Table Right	DnTABLE Access Level	Table	Tables
CXXMAINT.PURGE				
DBTEST				
DEFRAG				
EXTBKUP.DATA				
EXTEND.DATA	LOAD			X
EXTEND.IXX	OPER			X
EXTRACT		READ	X	
ENCRYPT				
FLEXPOOL.ADD				
FLEXPOOL.DELETE				
INIT.CXX				
INIT.DATA	LOAD			X
INIT.IXX	OPER			X
INIT.LXX				
INIT.WXX				
LINK	CATALOG			X
LOAD.CXX				
LOAD.CXXBASE	CATALOG			X
LOAD.DATA	LOAD			X
LOCK.MOVER	OPER			X
MASSADD		ADD	X	
OLREORG				
RECOVERY.BACKWARD	LOAD			X
RECOVERY.FORWARD	LOAD			X
REMOVE	CATALOG			X
REORG.DATA	BACKUP LOAD			X
REPLACE.DATA	LOAD		X	
REPORT.CXX	DISPLAY			X

DTUTIL Function and Sub Function	DTUTIL Table Right	DnTABLE Access Level	Table	Tables
REPORT.DEVICE				
REPORT.DDNAME				
REPORT.ENCRYPT				
REPORT.HISTORY	DISPLAY			X
REPORT.IXX	DISPLAY			X
REPORT.IXXDUMP		READ		X
REPORT.LXX				
REPORT.PXX				
REPORT.REFGROUP		READ	X	
REPORT.RXX				
RESET.CXX	OPER			X
RESET.LXX				
RETIX	OPER			X
RXXFIX				
SECURITY.RESET				
SPILL				
SPILLREW				
SPLIT				
UNLOCK.MOVER	OPER			X
VERINDEX				

***** For more information about AUTO DBUTLTYs, see the following Valid DBUTLTY External Security Rights table.

Valid DBUTLTY External Security Rights

DTUTIL Function and Sub Function	Access Level to Dyn. Systems Tbls	Access Level to Auto Tables
AUTOCOLL.AVGPERF		READ and ADD
AUTOCOLL.BASELINE		READ and ADD
AUTOCOLL.DELTACRE	READ	ADD

DTUTIL Function and Sub Function	Access Level to Dyn. Systems Tbls	Access Level to Auto Tables
AUTOCOLL.DELTADEL		READ and DELETE
AUTOCOLL.DELTARPT		READ
AUTOCOLL.DSVOUT		READ
AUTOCOLL.SNAPDEL		READ and DELETE
AUTOCOLL.SNAPRPT		READ
AUTOCOLL.SNAPSHOT	READ	ADD
AUTOCOLL.SUMMARY		READ and ADD
AUTOINFOTOR	READ	
AUTOSTAT		ADD

Examples

DBMUF001.DBUTLTY.ACCT.CATALOG validates the right of a requestor to perform the subfunction CATALOG of the DBUTLTY function ACCT to catalog the Accounting Facility database in the system known as DBMUF001. This requires OPER access rights for all user-defined Accounting tables and the PRM table.

DBMUF001.DBUTLTY.INIT.CXX validates the right of a requestor to perform the DBUTLTY function INIT CXX in the system known as DBMUF001.

DBMUF001.DBUTLTY.MASSADD validates the right of a requestor to perform the DBUTLTY function MASSADD in the system known as DBMUF001. This requires the ADD access level for the table where the records are added.

DBUTLTY Functions and Multi-User Facility Not Active

If the MUF is not active and non-SQL security is installed, most DBUTLTY functions are denied with a return code 68. The following functions execute and run as if security is not installed:

Description	Functions
Full CXX Maintenance	INIT AREA=CXX LOAD AREA=CXX,DDNAME=aaaaaaaa (with no DBID specified) CXXMAINT OPTION=CONVERT
Reporting	REPORT AREA=PXX REPORT DEVICE=
Recovery	RESET AREA=CXX,DBID=database-identifier

Logging	INIT AREA=LXX INIT AREA=FXX INIT AREA=WXX RESET AREA=LXX
Miscellaneous	TESTDATA EDIT

Note: TESTDATA is used at installation to load the files used in the DEMO database.

If you specify the CXX in your JCL, you *must* specify the same CXX used by the MUF, or return code 44 (an environment error) is issued.

CA Datacom Datadictionary and External Security

When external security is in effect, the CA Datacom Datadictionary Service Facility (DSF) determines the following at user signon from CAISSF:

- The identity of the user
- All CA Datacom Datadictionary facilities for which the user is authorized
- Whether the user is authorized as an administrator

Identify the CA Datacom Datadictionary facilities and functions by entity-type and status using the DTUTIL resource class to secure them with external security. Identify the Security Administrator using the DTADMIN resource class. For more information about externally securing CA Datacom Datadictionary online signons, see Enabling Online Signons (see page 61).

Internal Overrides

There are CA Datacom Datadictionary rules that cannot be overridden by external security.

- A history (HIST) status entity-occurrence can be displayed, copied from, obsoleted, and deleted only. Therefore, any attempt to update any entity-occurrence in HIST status is rejected by DSF regardless of the information provided by the call to CAISSF. (This is true for CA Datacom Datadictionary product security profiles also.)
- CA Datacom Datadictionary entity-occurrence definitions that are defined with password or lock level protection cannot be updated without supplying the assigned password or code. For more information about assigning, using, and deleting passwords and lock levels, see the CA Datacom Datadictionary documentation.
- Field definitions using the DDUPDATE 4099 Field Access transaction maintain attribute-level security.

If the user is identified as an internal CA product such as CA Dataquery or CA Ideal, DSF bypasses security checks (except CA Datacom Datadictionary entity-occurrence passwords and locks). For example, USERA is not authorized to use CA Datacom Datadictionary. When USERA uses CA Ideal, CA Ideal is still able to make the DSF calls needed to accomplish its work on behalf of USERA because CA Ideal signs on as an internal CA product. However, if USERA tries to execute a user program through CA Ideal that makes DSF calls, USERA is denied access to CA Datacom Datadictionary.

If external security is not in effect, CA Datacom Datadictionary uses any security information, including user profiles and System Resource Table (SRT) security options, that are defined through internal CA Datacom Datadictionary security.

DTADMIN Resource Class

The DTADMIN class is used to associate system product combinations with those individuals who have product administrator authority. This class indicates users with Security Administrator status.

DBMUF001.DD is an example of a DTADMIN resource for CA Datacom Datadictionary. Any users associated with this resource would be considered to be a Security Administrator to the CA Datacom Datadictionary.

DTUTIL Resource Class

The DTUTIL class is used to identify user access, the CA Datacom Datadictionary facilities, and the functions by entity-type and status that users are allowed to execute. This section provides the syntax for the DTUTIL resource class for CA Datacom Datadictionary.

In the following formats, cxxname represents the Directory (CXX) name and nnnn in DD0nnnn represents the database ID for the DATA-DICT database for CA Datacom Datadictionary.

User Access

The following format is used to authorize a CA Datacom Datadictionary user to access CA Datacom Datadictionary online and submit batch utility transactions (the -USR transaction). You must also perform the steps specified in Enabling Online Signons (see page 61).

```
cxxname.DD0nnnn.SIGNON
```

Facilities Resource List

The following formats for the DTUTIL resource class correspond to the CA Datacom Datadictionary facilities security formats used in the internal CA Datacom Datadictionary security.

Format Description

cxxname.DD0nnnn.DDOL.AUTH

Online Authorization Maintenance

cxxname.DD0nnnn.DDOL.DBM

Online CA Datacom/DB Structure Maintenance

cxxname.DD0nnnn.DDOL.ENTD

Online Entity Display

cxxname.DD0nnnn.DDOL.ENTM

Online Entity Maintenance

cxxname.DD0nnnn.DDOL.FMM

Online FILE Structure Maintenance

cxxname.DD0nnnn.DDOL.ISF

Online Interactive Service Facility

cxxname.DD0nnnn.DDOL.SQL

Online Interactive SQL Service Facility

cxxname.DD0nnnn.DDBTGLM

Batch DDBTGLM

cxxname.DD0nnnn.DDCFBLD

Batch DDCFBLD

cxxname.DD0nnnn.DDRMFLM

Batch DDRMFLM

cxxname.DD0nnnn.DDTRSLM

Batch DDTRSLM

cxxname.DD0nnnn.DDUPDATE

Batch DDUPDATE

cxxname.DD0nnnn.DDUTILTY

Batch DDUTILTY

Example

DBMUF001.DD00002.DDOL.SQL validates the authorization of a requestor to use the Interactive SQL Service Facility in the online mode of a CA Datacom Datadictionary with database ID of 2 using a system known as DBMUF001.

Entity-Type Resource List

This form corresponds to the CA Datacom Datadictionary entity-type security. The same conventions used by CA Datacom Datadictionary online security are used to represent entity-types and functions. See the table in Valid Entity-Type and Function Combinations (see page 48) for valid entity-type, status, and function combinations.

`cxxname.DD0nnnn.table.stat.fnc`

fnc

A 2- or 3-character identifier of the CA Datacom Datadictionary function.

ADD

Add or create an entity-occurrence (except FIELD).

ALS

Maintain aliases for an entity-occurrence.

CAT

Catalog a DATABASE structure.

DEF

Define a FIELD entity-occurrence to a table or record.

DEL

Delete or remove an entity-occurrence (except FIELD).

DES

Maintain descriptors for an entity-occurrence.

DIS

Display an entity-occurrence.

DSA

Disable a structure.

ENA

Enable a structure.

FRM

Copy an entity-occurrence from this one.

OB

Obsolete a structure (remove all status/versions).

REL

Maintain relationships for or transfer an entity-occurrence.

RES

Restore an entity-occurrence to this version.

SEC

Maintain passwords and lock levels.

SET

Set default attribute-values for entity-occurrences in a DATABASE structure.

STA

Maintain status for an entity-occurrence.

TO

Copy an entity-occurrence to this status/version.

TXT

Maintain text for an entity-occurrence.

UPD

Update or modify an entity-occurrence.

VER

Verify DATABASE or FILE structures.

nnnnn

The DBID attribute-value of the DATA-DICT database.

stat

The status identifier for the entity-type. PROD is also used for entity-occurrences in qualified (QUAL) and HIST status. TEST or Tnnn is also used for entity-occurrences in INCOmplete status.

- The status can be PROD, TEST, or T001 to T999 for entity-occurrences of the entity-types in the CA Datacom/DB and CA FILE Model structures: DATABASE, AREA, TABLE, FIELD, KEY, ELEMENT, FILE, RECORD, and DATAVIEW.
- The status can be PROD or TEST for entity-occurrences of all entity-types.
- For the OBS function, use PROD for the status.

cxxname

The 1- to 8-character system identifier.

table

The 3-character DATACOM-NAME attribute-value of the table defining the entity-type in the CA Datacom Datadictionary DATA-DICT database.

The following are the entity-types supplied with CA Datacom Datadictionary:

Entity-Type CA Datacom Datadictionary Name	DATACOM-NAME
ALIAS	ALS
AREA	ARA
AUTHORIZATION	ATZ
CONSTRAINT	CNS
DATABASE	BAS
DATAVIEW	DVW
DESCRIPTOR	KWC
ELEMENT	ELM
FIELD	FLD
FILE	FIL
JOB	JOB
KEY	KEY
LIBRARY	LIB
MEMBER	MEM
MODULE	MOD
NODE	NOD

PANEL	PNL
PARTITION-COLUMN-VALUE	PCV
PARTITION-VALUE	PRT
PARAMETER-LIST	PRM
PERSON	PER
PLAN	PLN
PROCEDURE	PRC
PROGRAM	PGM
RECORD	REC
RELATIONSHIP	REL
REPORT	RPT
STATEMENT	STM
STEP	STP
SYNONYM	SYN
SYSTEM	SYS
TABLE	TBL
TEXT	TXT
TRIGGER	TRG
UNIVERSAL (record)	UNI
VIEW	VEW

Valid Entity-Type and Function Combinations

The following chart shows the valid combination of entity-types, status, and functions that can be used in constructing CA Datacom Datadictionary resources. Most invalid function and entity-type combinations are ignored. For example, CA Datacom Datadictionary does not prevent you from assigning the SET function to the PROGRAM entity-type, but CA Datacom Datadictionary would not select it because SET is not a valid function for a PROGRAM entity-occurrence.

Entity-Type CA Datacom Datadictionary Name	**Table DATACOM-NAME**	**Status**	**Valid Functions**
ALIAS	ALS	PROD TEST	ADD, DEL, DIS, UPD

Entity-Type CA Datacom Datadictionary Name	Table DATACOM-NAME	Status	Valid Functions
AREA	ARA	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, REL, TO, TXT, UPD
AUTHORIZATION	ATZ	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
CONSTRAINT	CNS	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
DATABASE	BAS	PROD TEST T001—T999	ADD, ALS, CAT, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, SET, TO, TXT, UPD, VER
DATAVIEW	DVW	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, TO, TXT, UPD
DESCRIPTOR	KWC	PROD TEST	ADD, DEL, DIS, UPD
ELEMENT	ELM	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, TO, TXT, UPD
FIELD	FLD	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
FILE	FIL	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, TO, TXT, UPD, VER
JOB	JOB	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
KEY	KEY	PROD TEST T001—T999	ADD, ALS, DEF, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, TO, TXT, UPD
LIBRARY	LIB	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
MEMBER	MEM	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
MODULE	MOD	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
NODE	NOD	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD

Entity-Type CA Datacom Datadictionary Name	Table DATACOM-NAME	Status	Valid Functions
PANEL	PNL	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PARAMETER-LIST	PRM	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
PARTITION-COLUMN-VALUE	PCV	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PARTITION-VALUE	PRT	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PERSON	PER	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PLAN	PLN	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
PROCEDURE	PRC	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
PROGRAM	PGM	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
RECORD	REC	PROD TEST T001—T999	ADD, ALS, DEF, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, TO, TXT, UPD
RELATIONSHIP	REL	PROD TEST	ADD, DEL, DIS, UPD
REPORT	RPT	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
STATEMENT	STM	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
STEP	STP	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
SYNONYM	SYN	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
SYSTEM	SYS	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
TABLE	TBL	PROD TEST T001—T999	ADD, ALS, DEF, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, SET, TO, TXT, UPD

Entity-Type CA Datacom Datadictionary Name	Table DATACOM-NAME	Status	Valid Functions
TEXT	TXT	PROD TEST	ADD, DEL, DIS, UPD
TRIGGER	TRG	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
UNIVERSAL (record)	UNI	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
user-defined entity-type	ccc	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
VIEW	VEW	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD

Example

DBMUF001.DD00002.BAS.PROD.CAT is an example of a DTUTIL resource for CA Datacom Datadictionary entity-type security. This validates the requestor's permission to catalog a DATABASE entity-occurrence definition in production (PROD) status in a CA Datacom Datadictionary with a database ID of 2 using a system known as DBMUF001.

Replication of Internal CA Datacom Datadictionary Security Levels

CA Datacom Datadictionary internal security uses the SECLVL= parameter of the System Resource Table (SRT) to indicate the level of security desired. These levels of security are represented by options 0 through 4. For more information, see Planning for CA Datacom Datadictionary Security (see page 106).

If your external security package allows you to use fixed-position character substitution, or "wildcards," when defining resource names, you can reduce the number of resource definitions when replicating a CA Datacom Datadictionary security level. These wildcards are represented by cc, ccc, or cccc in the following examples. If the product allows variable character substitution, or "masking," you can use it as appropriate in place of wildcards. If the product does not use wild cards or masking you must specify each combination of entity-type, status, and function. CA Datacom Datadictionary rules cannot be overridden by using the substitution or patterning techniques in an external security product.

Level 0

Level 0 is the least restrictive. The only requirement is that the user is defined to the CA Datacom Datadictionary. At this level, each user can access any CA Datacom Datadictionary utility and can perform all valid functions on any TEST status or INCOmplete status entity-occurrence, and can perform the DISPLAY and RESTORE functions on any PROD status or HIST status entity-occurrence.

To emulate this class externally, the user must be authorized to use the CA Datacom Datadictionary. All users must have the following defined to the DTUTIL Resource Class:

```
cxxname.DD0nnnn
```

Level 1

Level 1 adds to the least restrictive level the requirement that the list of CA Datacom Datadictionary utilities be customized for each user. At this level, each user can perform all valid functions on any TEST status or INCOmplete status entity-occurrence, and can perform the DISPLAY and or RESTORE functions on any PROD status or HIST status entity-occurrence.

To emulate this class externally, the user must be authorized to use the CA Datacom Datadictionary (SIGNON). The specific permitted DDOL functions and batch utilities must be provided. The user would have the following defined to the DTUTIL Resource Class. For more information, see Valid Entity-Type and Function Combinations (see page 48).

```
cxxname.DD0nnnn.SIGNON
cxxname.DD0nnnn.DDOL.AUTH
cxxname.DD0nnnn.DDOL.DBM
cxxname.DD0nnnn.DDOL.ENTD
cxxname.DD0nnnn.DDOL.ENTM
cxxname.DD0nnnn.DDOL.FMM
cxxname.DD0nnnn.DDOL.ISF
cxxname.DD0nnnn.DDOL.SQL
cxxname.DD0nnnn.DDBTGLM
cxxname.DD0nnnn.DDCFBLD
cxxname.DD0nnnn.DDRMFLM
cxxname.DD0nnnn.DDTRSLM
cxxname.DD0nnnn.DDUPDATE
cxxname.DD0nnnn.DDUTILTY

cxxname.DD0nnnn.ccc.TEST.cc      (This is for the TO function.)
cxxname.DD0nnnn.ccc.TEST.ccc     (All other functions are three characters.)
cxxname.DD0nnnn.ccc.PROD.DIS
cxxname.DD0nnnn.ccc.PROD.RES
```

Level 2

Level 2 adds to Level 1 the requirement that each entity-type must be defined for the specific user. At this level, each user can perform all valid functions on any TEST status or INCOmplete status entity-occurrence, and can perform the DISPLAY and or RESTORE functions on any PROD status or HIST status entity-occurrence.

To emulate this class externally, the user must be authorized to use the CA Datacom Datadictionary (SIGNON). The specific permitted DDOL functions and batch utilities must be provided as in Level 1. Additionally, for each defined entity-type, the statements in the following format must be provided. For more information, see Valid Entity-Type and Function Combinations (see page 48):

```
cxxname.DD0nnnn.table.TEST.cc      (This is for the TO function.)
cxxname.DD0nnnn.table.TEST.ccc     (All other functions are three characters.)
cxxname.DD0nnnn.table.PROD.DIS
cxxname.DD0nnnn.table.PROD.RES
```

Level 3

Level 3 adds to Level 2 the requirement that the status for each defined entity-type must be provided. At this level, each user can perform any function for the entity-occurrences that have the entity-type and status specified.

To emulate this class externally, the user must be authorized to use the CA Datacom Datadictionary (SIGNON). The specific permitted DDOL functions and batch utilities must be specified as in Levels 1 and 2. Additionally, each defined entity-type must be described using the following formats. For more information, see Valid Entity-Type and Function Combinations (see page 48).:

```
cxxname.DD0nnnn.table.stat.cc      (This is for the TO function.)
cxxname.DD0nnnn.table.stat.ccc     (All other functions are three characters.)
```

Level 4

Level 4 is the most restrictive. The function must be provided for each defined entity-type. At this level, each user can only perform the valid functions for an entity-occurrence that has the entity-type, status, and function specified.

To emulate this class externally, the user must be authorized to use the CA Datacom Datadictionary (SIGNON). The specific permitted DDOL functions and batch utilities must be provided as in Levels 1 through 3. Additionally, each defined entity-type must be described with the following format. For more information, see Valid Entity-Type and Function Combinations (see page 48).

```
cxxname.DD0nnnn.table.stat.fnc
```

Profiles

CA Datacom Datadictionary is installed with four profiles ($DD-ADM, $DD-COP, $DD-DIS, and $DD-UPD) that can be used with internal security. The following formats show the DTUTIL resources that must be defined to emulate the profiles.

If your external security package allows you to use fixed position character substitution, or "wildcards," when defining resource names, you can use them in place of the cc, ccc, or cccc in the following formats. If the product allows variable character substitution, or "masking", you can use it as appropriate in place of wildcards. CA Datacom Datadictionary rules cannot be overridden if you use these in your external security product. If the product does not allow character substitution, you must specify each combination of entity-type, status, and function. For more information, see Valid Entity-Type and Function Combinations (see page 48).

$DD-ADM Profile

This profile is for users with CA Datacom Datadictionary Administrator authority. The first resource is the DTADMIN resource to identify a Security Administrator. For more information, see Valid Entity-Type and Function Combinations (see page 48).

```
cxxname.DD

cxxname.DD0nnnn.SIGNON
cxxname.DD0nnnn.DDOL.AUTH
cxxname.DD0nnnn.DDOL.DBM
cxxname.DD0nnnn.DDOL.ENTD
cxxname.DD0nnnn.DDOL.ENTM
cxxname.DD0nnnn.DDOL.FMM
cxxname.DD0nnnn.DDOL.ISF
cxxname.DD0nnnn.DDOL.SQL
cxxname.DD0nnnn.DDBTGLM
cxxname.DD0nnnn.DDCFBLD
cxxname.DD0nnnn.DDRMFLM
cxxname.DD0nnnn.DDTRSLM
cxxname.DD0nnnn.DDUPDATE
cxxname.DD0nnnn.DDUTILTY

cxxname.DD0nnnn.ccc.cccc.cc      (This is for the TO function.)
cxxname.DD0nnnn.ccc.cccc.ccc     (All other functions are three characters.)
```

$DD-COP Profile

This profile is for users with COPY authority. For more information, see Valid Entity-Type and Function Combinations (see page 48).

```
cxxname.DD0nnnn.SIGNON
cxxname.DD0nnnn.DDOL.DBM
cxxname.DD0nnnn.DDOL.ENTD
cxxname.DD0nnnn.DDOL.ENTM
cxxname.DD0nnnn.DDOL.FMM
cxxname.DD0nnnn.DDUPDATE
cxxname.DD0nnnn.DDUTILTY

cxxname.DD0nnnn.ccc.TEST.ADD
cxxname.DD0nnnn.ccc.TEST.ALS
cxxname.DD0nnnn.ccc.TEST.DEF
cxxname.DD0nnnn.ccc.TEST.DEL
cxxname.DD0nnnn.ccc.TEST.DES
cxxname.DD0nnnn.ccc.TEST.FRM
cxxname.DD0nnnn.ccc.TEST.REL
cxxname.DD0nnnn.ccc.TEST.SET
cxxname.DD0nnnn.ccc.TEST.TO
cxxname.DD0nnnn.ccc.TEST.TXT
cxxname.DD0nnnn.ccc.TEST.UPD
cxxname.DD0nnnn.ccc.TEST.VER
cxxname.DD0nnnn.ccc.cccc.DIS
```

$DD-DIS Profile

This profile is for users with DISPLAY authority only. For more information, see Valid Entity-Type and Function Combinations (see page 48).

```
cxxname.DD0nnnn.SIGNON
cxxname.DD0nnnn.DDOL.ENTD
cxxname.DD0nnnn.DDOL.SQL
cxxname.DD0nnnn.DDUTILTY

cxxname.DD0nnnn.ALS.cccc.DIS
cxxname.DD0nnnn.ARA.cccc.DIS
cxxname.DD0nnnn.ATZ.cccc.DIS
cxxname.DD0nnnn.BAS.cccc.DIS
cxxname.DD0nnnn.DVW.cccc.DIS
cxxname.DD0nnnn.KWC.cccc.DIS
cxxname.DD0nnnn.ELM.cccc.DIS
cxxname.DD0nnnn.FLD.cccc.DIS
cxxname.DD0nnnn.FIL.cccc.DIS
cxxname.DD0nnnn.JOB.cccc.DIS
cxxname.DD0nnnn.KEY.cccc.DIS
cxxname.DD0nnnn.LIB.cccc.DIS
cxxname.DD0nnnn.MEM.cccc.DIS
cxxname.DD0nnnn.MOD.cccc.DIS
cxxname.DD0nnnn.NOD.cccc.DIS
cxxname.DD0nnnn.PER.cccc.DIS
cxxname.DD0nnnn.PGM.cccc.DIS
cxxname.DD0nnnn.PNL.cccc.DIS
cxxname.DD0nnnn.PRT.cccc.DIS
cxxname.DD0nnnn.REC.cccc.DIS
cxxname.DD0nnnn.REL.cccc.DIS
cxxname.DD0nnnn.RPT.cccc.DIS
cxxname.DD0nnnn.STP.cccc.DIS
cxxname.DD0nnnn.SYS.cccc.DIS
cxxname.DD0nnnn.TBL.cccc.DIS
cxxname.DD0nnnn.TXT.cccc.DIS
cxxname.DD0nnnn.UNI.cccc.DIS
```

$DD-UPD Profile

This profile is for users with UPDATE authority. For more information, see Valid Entity-Type and Function Combinations (see page 48).

```
cxxname.DD0nnnn.SIGNON
cxxname.DD0nnnn.DDOL.DBM
cxxname.DD0nnnn.DDOL.ENTD
cxxname.DD0nnnn.DDOL.ENTM
cxxname.DD0nnnn.DDOL.FMM
cxxname.DD0nnnn.DDUPDATE
cxxname.DD0nnnn.DDUTILTY

cxxname.DD0nnnn.ccc.TEST.ADD
cxxname.DD0nnnn.ccc.TEST.ALS
cxxname.DD0nnnn.ccc.TEST.DEF
cxxname.DD0nnnn.ccc.TEST.DES
cxxname.DD0nnnn.ccc.TEST.REL
cxxname.DD0nnnn.ccc.TEST.SET
cxxname.DD0nnnn.ccc.TEST.TXT
cxxname.DD0nnnn.ccc.TEST.UPD
cxxname.DD0nnnn.ccc.TEST.VER
cxxname.DD0nnnn.ccc.cccc.DIS
```

CA Dataquery and External Security

If external security is active on the system, CA Dataquery obtains the signon ID of the user from the external security package. Once the signon ID is retrieved, CA Dataquery checks the eligibility of the user to sign on to CA Dataquery. To leave off the signon card in batch, you must also specify SECINF=YES in the DQOPTLST.

After CA Dataquery determines that a user is eligible for signon, CA Dataquery makes additional resource checks to determine the access of the user to functions from external security. If a DQU record for the user exists, the record is updated with the latest access rights from external security. If one does not exist, one is created, since the DQU record also contains various profile options maintainable by the individual user.

The access rights in effect at the beginning of a CA Dataquery session determine the functions appearing on CA Dataquery menus and the commands allowed throughout the CA Dataquery session. When an externally secured function is requested by command or PF key or from a menu, the function is checked to determine if the user is still authorized.

If external security is not in effect, CA Dataquery internal security is in effect.

Internal Overrides

If secured within CA Dataquery, column-level security functions, profile codes, and condition/restriction are in effect regardless of whether they are externally secured.

Implementation of external security in CA Dataquery allows the Security Administrator to define user rights to perform the CA Dataquery functions and to execute the CA Dataquery batch utility functions using the external security definitions of the user. External security for data (CA Datacom/DB tables) is provided through CA Datacom/DB. When external security is in effect on the system, the signon ID is retrieved from the external security product in both online and batch mode and in the batch utilities.

CA Dataquery uses the DTUTIL class to identify CA Dataquery functions and the users allowed to execute them. The functions have the same names and the same meaning as those implemented by CA Dataquery online security.

CA Dataquery Resource List

The DTUTIL resource class has portions of the resource name defined by functions in CA Dataquery. The following is a list of valid CA Dataquery DTUTIL resources. Replace cxxname with the appropriate Directory (CXX) name.

Note: If the cxxname.DQACCESS.CONVUSER ACCESS(ALL) resource is present, the user is identified as a "Conventional User."

If the cxxname.DQACCESS.CONVUSR ACCESS(NONE) resource is present, or if the CONVUSR keyword authorization is absent, the user is identified as an "Associate User," meaning that the user is allowed to run existing queries only.

CA Dataquery Resource Name Formats for DQACCESS

- cxxname.DQACCESS.CONVUSR
- cxxname.DQACCESS.DQLSQL
- cxxname.DQACCESS.EMAIL
- cxxname.DQACCESS.EXPORT
- cxxname.DQACCESS.PDB
- cxxname.DQACCESS.REPORT
- cxxname.DQACCESS.SQLDDL
- cxxname.DQACCESS.SQLDML
- cxxname.DQACCESS.SUBMIT

CA Dataquery Resource Name Formats for DQADMIN

- cxxname.DQADMIN.ACTUSER
- cxxname.DQADMIN.COND
- cxxname.DQADMIN.DIAG
- cxxname.DQADMIN.JCL
- cxxname.DQADMIN.LANGUAGE
- cxxname.DQADMIN.LIBRARY
- cxxname.DQADMIN.PRINTER
- cxxname.DQADMIN.REST
- cxxname.DQADMIN.SECURITY
- cxxname.DQADMIN.SETS
- cxxname.DQADMIN.USER

CA Dataquery Resource Name Formats for DQCRRPT

- cxxname.DQCRRPT.REPORT

CA Dataquery Resource Name Formats for DQLANGMT

- cxxname.DQLANGMT.LOAD
- cxxname.DQLANGMT.UNLOAD (includes UPSHIFT)

CA Dataquery Resource Name Formats for DQLIBRMT

- cxxname.DQLIBRMT.ADD
- cxxname.DQLIBRMT.BACKUP
- cxxname.DQLIBRMT.REMOVE
- cxxname.DQLIBRMT.REPORT
- cxxname.DQLIBRMT.RESTORE

CA Dataquery Resource Name Formats for DQPANPRT

- cxxname.DQPANPRT.PRINT

CA Dataquery Resource Name Formats for DQSIGNON

- cxxname.DQSIGNON

CA Dataquery Resource Name Formats for DQUSERMT

- cxxname.DQUSERMT.ADD
- cxxname.DQUSERMT.DELETE

- cxxname.DQUSERMT.REPORT
- cxxname.DQUSERMT.UPDATE

CA Dataquery Resource Name Formats for DQWFINIT

- cxxname.DQWFINIT.DQE
- cxxname.DQWFINIT.DQF
- cxxname.DQWFINIT.DQW

Example

DBMUF001.DQACCESS.DQLSQL validates the right of a requestor to use the SQL Mode of CA Dataquery using a system known as DBMUF001. (It is not necessary to specify a CA Datacom Datadictionary ID.)

Table Authorizations

When external security is in effect, CA Dataquery checks with CA Datacom/DB to determine if you are authorized to access a particular table. The indication of access allowed or not allowed is the only factor used by CA Dataquery for table security. All CA Dataquery table security is ignored.

When external security is not in effect, access to tables is governed by CA Dataquery as documented in DQ Internal Security (see page 187).

PDB and STORE Considerations

Here are some considerations for the use of PDB (personal data base) and the STORE command. With these functions and by using SQL, tables are created in an area specified in your profile (this profile information is still used even when external security is in effect for CA Dataquery). The area must be in a database for which you have both create authority and CA Dataquery authority to do maintenance. The area and database should be built separately for each user or group of users that are allowed PDB authority, so that these tables are not put into any arbitrary database.

Note: For more information about how to set up a database for SQL use, see the *CA Datacom/DB Database and System Administration Guide*.

When external security is in effect, you must have full access rights to the database where personal tables are created (for PDB or STORE). This includes CREATE and DROP authority, that is, cxxname.DBdbid.999.CATALOG. This is the reason that we recommend separate databases for each group of users that can have access to each other's tables. The authority to specify in the external security package is cxxname.DBdbid (with required generics) to allow PDB and STORE to function properly.

Note: For more information about using PDB, see the *CA Dataquery Administrator Guide*.

CA Dataquery Batch Utility Functions

When external security is in effect, CA Dataquery obtains the signon ID of the user from external security and determines if the user is eligible to sign on to CA Dataquery. If not, the utility execution is terminated. Only the signon ID from external security is used. If the user is eligible, CA Dataquery determines which functions the user is authorized to perform. If a function is requested for which the user is not authorized, an error message prints.

Note: For more information about how the batch utilities function when external security is not in effect, see the *CA Datacom/DB Database and System Administration Guide*.

Enabling Online Signons

The following steps can be used as a guide to enable external security for online signons to CA IPC based products and facilities such as CA Datacom Datadictionary online and CA Ideal. For sites that use external security to validate signons, you must use the SC00OPTS SECRTY=Y option over the traditional method which extracts the user ID from the value present in the TCTTEOI of the CICS TCTTE when SC00OPTS SECRTY=N.

Note: For information about coding SC00OPTS, see Step 6 and the *CA IPC Implementation Guide*.

Step 1

Ensure that CAISSF has been installed.

In z/OS sites, CAISSF is a subservice of the CAIRIM, a component of the CA Common Services for z/OS. Additionally, RACF users must follow the instructions for customizing CAISSF for RACF and RACF-compatible products in the CA Common Services for z/OS installation guide. CAS9SAFC must be assembled with CICS-YES if RACF is installed.

In z/VSE sites, CAISSF is a separate service of the CA CIS. See the CA CIS installation guide.

Step 2

Define the CA Command resource class in the security product. For CA ACF2 and CA Top Secret, the resource class should already be present.

Product	CA Command Resource Class Name
CA ACF2	CAC
CA Top Secret	CACMD
RACF	CA@MD (by default) (see the *CA Common Services for z/OS Installation Guide*

Step 3

Authorize users for access to the CA Command resource for the SCF-based product or component of the product they need to access.

Product or Component	Value of CA Command Resource
CA Datacom Datadictionary	DDSIGNON
CA Ideal	*sp*SIGNON, where *sp* is the 2-character SECPRFX assigned in IDOPTS.
CA IPC	IPSIGNON

For more information, see Sample CA Command Resource Definitions (see page 65).

Step 4

Define the "partition job card user" in the external security product if job submits take place. This has nothing to do with the SC00OPTS security option being set to yes, but what the security package is put into the job statement when a job is submitted through the TP monitor. For example, under CICS, CA Top Secret can be set to put the CICS user name and password into the job statement parameters.

At this point, establish the user access for each CA Datacom Datadictionary user. For more information, see User Access (see page 43).

Step 5

For CA Ideal, establish a link between the security ID and user ID using one of the following methods. For other products, however, if you want to return to internal product security, we recommend that you keep the users in CA Datacom Datadictionary in synch with the external users you have enabled with CA Datacom Datadictionary authority using one of these methods.

- The CA Datacom Datadictionary or CA Ideal user name can match the security ID. If this is not already true, it is possible to modify existing user definitions by changing long names to match security ID names. This can be done using the CA Datacom Datadictionary DDUPDATE utility. However, it does require that all TEST and HIST status versions of the PERSON (USERS) entity-occurrence be deleted first.

  To change the person names, you can simply run the following transactions in a single DDUPDATE batch job. Use a set of these transactions for each PERSON entity-occurrence name you want to change. If you have a file of the old and new names, you could write a quick program to generate the transactions for you.

  ```
  -UPD PERSON,old-name(PROD,,ovrd)
  1000 NEWNAME,newname
  -END
  ```

  Note: This method modifies the CA Datacom Datadictionary user signon definition, but not the CA Dataquery user in entirety.

- If users are already defined and the security ID does not match the current user ID, add a CA Datacom Datadictionary alias to the PERSON entity-occurrence equal to the security ID. Aliases can easily be added in a single batch job executed in the CA Datacom Datadictionary DDUPDATE utility. The PROD status version of the PERSON entity-occurrences can be updated.

- Use the DFLTUSR option in SC00TRAN on a transaction basis. Under CA Ideal, it is also available in IDOPTS as an environment option. If a default user is specified for the transaction, it takes precedence over a default user specified in IDOPTS. This is only a viable alternative if the CA Ideal user definition used to sign on does not need to be known.

For CA Ideal, consider the impact the option you choose is going to have on the $USER-NAME or $USER-ID functions that may exist in CA Ideal programs. The values may be different depending on the method of implementation. In some cases, the new value may be the desired result, while others may require modification to existing CA Ideal applications or other applications that are accessing data CA Ideal may be updating. The most important fact to realize is that the values returned for $USER functions reflect the CA Ideal user definition used for signon and not the security ID or alias.

For CA Datacom Datadictionary, when a new user of online (who has authorization for the facility) attempts access to the Interactive SQL Service Facility, CA Datacom Datadictionary automatically places a PERSON entity-occurrence in CA Datacom Datadictionary that matches the security ID to tie the SQL default AUTHID to it.

Step 6

Reassemble SC00OPTS with SECRTY=Y. (For more information about coding SC00OPTS, see the *CA IPC Implementation Guide.)*

Step 7

For CA Ideal, reassemble IDOPTS for each region where a different SECPRFX is desired (UIDCHK and PSWCHK options in IDOPTSCB should be no as they are ignored when the security ID is extracted).

Step 8

Optionally in CICS, remove the user ID from SNT.

Step 9

CICS tables may need to be modified depending on the security product.

Step 10

To ensure unique signons, secure through the external security product. Optionally, you can use the CA IPC SET SITE option to check for duplicates. See the CA IPC documentation for details.

Step 11

Optionally, issue SET SITE ASYNCMSG for the region to suppress network print and compile messages that may not belong to the user if the CA IPC Print SubSystem (PSS) is active or CA Ideal is installed.

Step 12

If the CA Datacom Datadictionary or CA Ideal users are defined with passwords, you must set the System Resource Table (DDSYSTBL macro) parameter EXPBYPP=YES.

Sample CA Command Resource Definitions

Important! The following information is not intended to replace nor supersede any information in the CA ACF2 and CA Top Secret documentation for the version being executed. The samples are not intended to display all features of the external security product. The specific rules provided are examples and are not intended as guidelines for establishing a secured environment.

CA ACF2 Example

See the CA ACF2 documentation for the appropriate syntax for the version installed at your site.

```
SET RESOURCE(CAC)
$KEY($ISIGNON) TYPE(CAC) UID(userid) ALLOW
$KEY(DBSIGNON) TYPE(CAC) UID(userid) ALLOW
$KEY(DDSIGNON) TYPE(CAC) UID(userid) ALLOW
$KEY(IPSIGNON) TYPE(CAC) UID(userid) ALLOW
```

CA Top Secret z/OS and z/VSE Example

For CA Ideal, users must be authorized for access to CACMD(spSIGNON) where sp is the two-character SECPRFX assigned in IDOPTS. See the CA Top Secret documentation for the appropriate syntax for the version installed at your site.

```
TSS CREATE(DEVL) TYPE(PROFILE) DEPT(DEVELOP)
    NAME('DEVELOPMENT DEPARTMENT AUTHORITY')
TSS ADD(DEVELOP) CACMD(DBSIGNON)
TSS ADD(DEVELOP) CACMD(DDSIGNON)
TSS ADD(DEVELOP) CACMD(IDSIGNON)
TSS ADD(DEVELOP) CACMD(IPSIGNON)
TSS PER(DEVL) CACMD(DBSIGNON)
TSS PER(DEVL) CACMD(DDSIGNON)
TSS PER(DEVL) CACMD(IDSIGNON)
TSS PER(DEVL) CACMD(IPSIGNON)
TSS CRE(USERA) TYPE(USER) DEPT(DEVELOP)
    NAME('A USER') PROFILE(DEVL) PASSWORD(USRPASS,30,EXPIRED)
    FACILITY(CICS)
```

Security Interfaces, CA-ACF2 (z/OS and z/VSE)

Caution: CA ACF2 is a "closed" system, that is, the default is to deny all access. All new systems are secured until permissions are specified. Permissions must be in place for all CA Datacom/DB activities before the CA Datacom/DB Directory initialization. For more information, see Activating External Security (see page 73).

Since the CA Datacom resources are defined as resident in CA ACF2, perform a recycle, or "rebuild," of the external security session if a change is made.

Sample ACF2 REBUILD command:

```
F ACF2,REBUILD(ttt)           ttt is the TYPE code for the resource
```

Limited Documentation

The following information is not intended to replace nor supersede any information in the CA ACF2 documentation for the version being executed. The samples are not intended to display all features of CA ACF2. The specific rules provided in the following resource classes are examples only and are not intended as guidelines for establishing a secured environment.

Defining Resources

CA ACF2 translates eight-character resource classes into three-byte CA ACF2 resource type codes using CA ACF2 GSO CLASMAP records. The documented CA Datacom resources DTSYSTEM, DTADMIN, DTTABLE, and DTUTIL are processed by default by CA ACF2 using the first three characters of the resource names: DTS, DTA, D*c*T, and DTU unless there is a matching CLASMAP entry that translates (maps) the resource class to a specific three-byte resource type.

```
*DcTABLE - DTTABLE - DTT
           DCTABLE - DCT
           DFTABLE - DFT
           DGTABLE - DGT
           DHTABLE - DHT
           DPTABLE - DPT
           DQTABLE - DQT
           DRTABLE - DRT
           DSTABLE - DST
           DXTABLE - DXT
```

For more information about these CA Datacom resources, see Setting Up Resource Classes (see page 24). If the CA Datacom resource rules contain masking in the $KEY, the CA ACF2 resource type must be made resident. Defining the resource types in the GSO INFODIR as follows can accomplish this:

```
SET CONTROL(GSO)
CHANGE INFODIR TYPES(R-RDTA,R-RDTU,R-RDCT,R-RDFT,R-RDRT,R-RDST,R-RDTT,R-RDXT) ADD
F ACF2,REFRESH(INFODIR)
```

Some sites may have a site defined CLASMAP for a resource class mask "********" mapping to a TYPE code of SAF. In this case, the default for undefined resource classes is SAF rather than the first three characters of the resource class. To override this specific CLASMAP, entries should be added for each CA Datacom resource class.

```
SET CONTROL (GSO)
SET SYSID (sysid)
INSERT CLASMAP.qual RESOURCE(class) RSRCTYPE(typecode)
F ACF2,REFRESH(CLASMAP)
```

When changing GSO records, remember to issue the REFRESH command and subsequently any other appropriate commands, such as RELOAD, REBUILD, and so on.

In the example just shown, the following descriptions of the variables (the words in lower case letters) apply:

sysid

Specifies the four-character SYSID.

qual

Specifies a label up to nine characters appended to CLASMAP. The period shown in the example is optional but if used counts as one of the nine characters.

class

Specifies an explicit eight-character Resource Class from CLASS keyword on RACROUTE macro.

typecode

Specifies the explicit three-character Resource Type Code associated with the Resource Class. If not specified, CA ACF2 uses the first three characters of the RESOURCE as RSRCTYPE.

The following example shows what to code to override the CLASMAP resource class mask "********" to a TYPE code of DTS for the DTSYSTEM resource class:

```
SET CONTROL (GSO)
SET SYSID (SYS1)
INSERT CLASMAP.DTS RESOURCE(DTSYSTEM) RSRCTYPE(DTS)
F ACF2,REFRESH(CLASMAP)
```

Following is an example showing how to define the DTADMIN resource class:

```
SET CONTROL (GSO)
SET SYSID (SYS1)
INSERT CLASMAP.DTA RESOURCE(DTADMIN) RSRCTYPE(DTA)
F ACF2,REFRESH(CLASMAP)
```

Defining Users

The following are examples of how to define security entries to secure a system. They are not intended to portray all possible CA ACF2 capabilities and are for example only. For more information, see Enabling Online Signons (see page 61).

```
SET LID
INSERT USERA NAME(TEST USER 1) PASSWORD(PSWD1) TSO JCL JOB CICS
INSERT USERB NAME(TEST USER 2) PASSWORD(PSWD2) TSO JCL JOB CICS
INSERT USERC NAME(TEST USER 3) PASSWORD(PSWD3) TSO JCL
```

Defining Access Rights of a User

The following are examples of rules for securing various CA Datacom/DB utilities using CA ACF2. For details, see the documentation CA ACF2.

```
SET RESOURCE(DTU)
COMPILE
$KEY(PRODCXX) TYPE(DTU)
$USERDATA(CA Datacom rules for resource DTUTIL)
DBUTLTY.BACKUP.CXX     UID(USERA)  ALLOW
DBUTLTY.BACKUP.DATA   UID(USERA)  ALLOW
DBUTLTY.BACKUP.DATA   UID(USERB)  PREVENT
DBUTLTY.BACKUP.-  UID(USERC)  PREVENT
DBUTLTY.COMM.-  UID(USERA)  ALLOW
DBUTLTY.COMM.-  UID(*)  PREVENT
DBUTLTY.LOAD.- UID(USERA)  ALLOW
DBUTLTY.LOAD.- UID(USERB)  PREVENT
DBUTLTY.REPORT.- UID(*)  ALLOW
DB00001.PAY.LOAD UID(USERA)  ALLOW
DB00001.PAY.LOAD UID(USERB)  PREVENT
DB00001.PAY.BACKUP UID(USERA)  ALLOW
DB00999.- UID(USERC)  PREVENT
DB00999.- UID(*)  ALLOW
-  UID(*)  PREVENT

STORE
```

The following rules only allow USERA to create SQL schemas, drop tables, and have product administration authority for CA Datacom Datadictionary and CA Dataquery.

```
SET RESOURCE(DTA)
COMPILE
$KEY(PRODCXX) TYPE(DTA)
$USERDATA(CA Datacom rules for the Administrator)
-  UID(USERA)  ALLOW
-  UID(*)  PREVENT

STORE
```

For more information about the DTADMIN resource, see DTADMIN (see page 32).

Defining Access Rights to Tables

The following rules are examples for securing table access using CA ACF2.

There are ten possible CA Datacom resource classes that can control table access. They are defined with access levels of READ, ADD, UPDATE, or DELETE. For more information about CA Datacom tables and multiple access levels, see Table Classes (see page 32). These resource classes can be validated by CA ACF2 resource rules using the default type codes of DCT, DFT, DGT, DHT, DPT, DQT, DRT, DST, DTT, or DXT unless there is a matching CLASMAP entry that translates (maps) the resource class to a specific 3-byte resource type.

Note: Some sites may have a site defined CLASMAP for a resource mask "********" mapping to a TYPE code of SAF. In this case, the default for undefined resource classes is SAF rather than the first three characters of the resource class. To override this specific CLASMAP, entries can be added for each CA Datacom resource class.

The following are examples of the Table Resource Classes.

```
SET RESOURCE(DCT)
COMPILE
$KEY(PRODCXX) TYPE(DCT)
$USERDATA(CA Datacom rules for table access)
dbid.tablename   UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(READ,DELETE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,UPDATE)  PREVENT
dbid.tablename   UID(USERC)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
dbid.tablename.  UID(USERA)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.tablename   UID(USERB)  SERVICE(READ)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.-  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.-  UID(*)  ALL  PREVENT
-  UID(*)  ALLOW

STORE

SET RESOURCE(DTT)
COMPILE
$KEY(PRODCXX) TYPE(DTT)
$USERDATA(CA Datacom rules for table access)
DB00001.PAY  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
DB00001.PAY  UID(USERB)  SERVICE(READ,DELETE)  ALLOW
DB00001.PAY  UID(USERB)  SERVICE(ADD,UPDATE)  PREVENT
DB00001.PAY  UID(USERC)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
DB00001.PMF  UID(USERA)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
DB00001.PMF  UID(USERB)  SERVICE(READ)  ALLOW
DB00001.PMF  UID(USERB)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
DB00999.-  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
DB00999.-  UID(*)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
-  UID(*)  ALLOW

STORE
```

```
SET RESOURCE(DFT)
COMPILE
$KEY(PRODCXX) TYPE(DFT)
$USERDATA(CA Datacom rules for table access)
dbid.tablename   UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(READ,DELETE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,UPDATE)  PREVENT
dbid.tablename   UID(USERC)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
dbid.tablename.  UID(USERA)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.tablename   UID(USERB)  SERVICE(READ)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.-  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.-  UID(*)  ALL  PREVENT
-  UID(*)  ALLOW

STORE

SET RESOURCE(DRT)
COMPILE
$KEY(PRODCXX) TYPE(DRT)
$USERDATA(CA Datacom rules for table access)
dbid.tablename   UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(READ,DELETE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,UPDATE)  PREVENT
dbid.tablename   UID(USERC)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
dbid.tablename.  UID(USERA)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.tablename   UID(USERB)  SERVICE(READ)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.-  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.-  UID(*)  ALL  PREVENT
-  UID(*)  ALLOW

STORE

SET RESOURCE(DST)
COMPILE
$KEY(PRODCXX) TYPE(DST)
$USERDATA(CA Datacom rules for table access)
dbid.tablename   UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(READ,DELETE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,UPDATE)  PREVENT
dbid.tablename   UID(USERC)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
dbid.tablename.  UID(USERA)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.tablename   UID(USERB)  SERVICE(READ)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.-  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.-  UID(*)  ALL  PREVENT
-  UID(*)  ALLOW

STORE
```

```
SET RESOURCE(DXT)
COMPILE
$KEY(PRODCXX) TYPE(DXT)
$USERDATA(CA Datacom rules for table access)
dbid.tablename   UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(READ,DELETE)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,UPDATE)  PREVENT
dbid.tablename   UID(USERC)  SERVICE(READ,ADD,DELETE,UPDATE)  PREVENT
dbid.tablename.  UID(USERA)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.tablename   UID(USERB)  SERVICE(READ)  ALLOW
dbid.tablename   UID(USERB)  SERVICE(ADD,DELETE,UPDATE)  PREVENT
dbid.-  UID(USERA)  SERVICE(READ,ADD,DELETE,UPDATE)  ALLOW
dbid.-  UID(*)  ALL  PREVENT
-  UID(*)  ALLOW

STORE
```

Securing the MUF (DTSYSTEM)

At the startup of the MUF, when the LEVEL PASS and FAIL resource names are properly set up, the external security product is called with a series of resource names in the DTSYSTEM resource class.

These resource names have a high-level node of the *cxxname* followed by a low-level node or nodes representing a product or feature, for example, *cxxname*.DQ for CA Dataquery. If any level is selected at the startup of the MUF, *cxxname*.DD and *cxxname*.DQ are also checked. If access is denied for *cxxname*.DD, CA Datacom Datadictionary is externally secured. If access is denied for *cxxname*.DQ, CA Dataquery is externally secured. For more information about DTSYSTEM resources, see Using the DTSYSTEM. The following is an example of a rule to secure CA Datacom products and features:

```
SET RESOURCE(DTS)
COMPILE
$KEY(cxxname) TYPE(DTS)
$USERDATA(Rule to secure CA Dataquery and Datadictionary with CA ACF2 allow XCF)
DD-  UID(logonid)  PREVENT
DQ-  UID(logonid)  PREVENT
XCF-  UID(logonid)  ALLOW

STORE
```

This rule secures CA Datacom Datadictionary and CA Dataquery with CA ACF2 external security and allows access to the XCF facility (no external security). For a complete list of resource features and products and their corresponding resource names, see Setting Up Resource Classes (see page 24).

Note: The UID string should represent the user logon ID that starts the MUF. The *cxxname* is the system identifier of the CA Datacom/DB Directory (CXX) name unique to each MUF.

Activating External Security

When CA Datacom implements security features, it does so by implementing a level of security in the DTSYSTEM resource class. This resource class is defined for each CA ACF2 system, therefore we recommend that you define this resource class last (or after all other specifications are defined). A level consists of a pair of resource names in the DTSYSTEM resource class.

The resource names ACTIVATE.LEVEL*nn*.PASS and ACTIVATE.LEVEL*nn*.FAIL are validated against the logon ID associated with the CA Datacom MUF. If access is allowed to the PASS resource and access is denied for the FAIL resource, that level of security is considered in force (external security is active) and further checks are made based on the level. For more information regarding CA Datacom external security and security levels, see Process Overview (see page 26).

The following is an example of the step, which activates CA ACF2 external security for the CA Datacom system at LEVEL04. This activates CA ACF2 external security for CA Datacom/DB, CA Datacom Datadictionary, and CA Dataquery. It allows the MUF to make further checks to verify that the user attempting to access specific resources has the appropriate authority.

```
SET RESOURCE(DTS)
COMPILE
$KEY(ACTIVATE) TYPE(DTS)
$USERDATA(Rule to activate CA ACF2 security for CA Datacom)
LEVEL04.PASS  UID(logonid)  ALLOW
LEVEL04.FAIL  UID(logonid)  PREVENT

STORE
```

The following is an example of how to change the permission from denied to allowed for the CA Datacom system. This definition allows full access to CA Datacom/DB, CA Datacom Datadictionary, and CA Dataquery while you are completing your definitions.

```
SET RESOURCE(DTS)
COMPILE
$KEY(ACTIVATE) TYPE(DTS)
$USERDATA(Rule to suppress security)
LEVEL04.PASS  UID(logonid)  PREVENT
LEVEL04.FAIL  UID(logonid)  ALLOW

STORE
```

LEVEL04 represents the security level (LEVEL*nn* where *nn* can be 01 through 04). The *logonid* in these examples is the CA ACF2 UID string for the logon ID associated with the MUF address space.

For sites that have the logon ID that starts the MUF address space defined as NON-CNCL, the rules discussed previously have no effect on determining the use of CA ACF2 for external security for CA Datacom. To control the use of external security, use CA ACF2 SAFDEFs to return the proper return codes to CA Datacom/DB to enforce the desired level of security. For example, the following SAFDEFs are equivalent to the first example, on how to activate external security for CA Datacom/DB, CA Datacom Datadictionary, and CA Dataquery for all MUF address spaces, that have the NON-CNCL privilege:

```
SET CONTROL(GSO)
INSERT SAFDEF.DCFAIL FUNCRET(8) FUNCRSN(0) ID(DATACOMF) MODE(IGNORE)  -
  RACROUTE(REQUEST=AUTH,CLASS=DTSYSTEM,ENTITYX=ACTIVATE.LEVEL04.FAIL)  -
  RETCODE(8) USERID(********)
INSERT SAFDEF.DCPASS FUNCRET(0) FUNCRSN(0) ID(DATACOMP) MODE(IGNORE)  -
  RACROUTE(REQUEST=AUTH CLASS=DTSYSTEM,ENTITYX=ACTIVATE.LEVEL04.PASS)  -
  RETCODE(0) USERID(********)
```

When changing GSO records, remember to issue the REFRESH command and subsequently any other appropriate commands, such as RELOAD, REBUILD, and so on.

Path Security

The SECURITY Multi-User startup option has options related to path security. Path security allows you to identify security rules for different command paths.

The resource name syntax is DB*aabbb*. This is the format of a path security class-and-path option parameter, where DB is a constant. The *aa* represents valid class codes. These class codes correspond to the table classes defined in the external security system. The table classes must be defined before implementing path security in CA Datacom/DB. The *bbb* represents one of the ten valid path codes you can secure with path security. For a description of all ten paths, see Using the DTSYSTEM.

If a class-and-path is specified in the SECURITY Multi-User startup option, a security check is issued for the DTSYSTEM class with a resource name cxxname.class-and-path.The *class-and-path* name must exactly match the seven letters coded in the Multi-User startup option (DB*aabbb*).

If access is denied, this path is secured using the class-and-path specified. If access is granted, an error is returned and the MUF does not enable. For more information about path security, see Using the DTSYSTEM sub-section "SECURITY Multi-User Startup Option". The following is an example of coding the Multi-User startup option:

```
SECURITY DBDTSSR,DBDTRAT,DBDTSCI,DBDTRSR,DBDTSQL,DBDTRCI
```

The following rule secures all paths to the DTTABLE resource class with CA ACF2 and there is no security in place for the DFTABLE resource class.

```
SET RESOURCE(DTS)
COMPILE
$KEY(cxxname)  TYPE(DTS)
$USERDATA(Path Security Secure DTTABLE no security for DFTABLE
DBDT-  UID(logonid)  PREVENT
DBDF-  UID(logonid)  ALLOW

STORE
```

Security Interfaces, CA Top Secret (z/OS)

Supported Versions

CA Top Secret z/OS Version 5.0 and later support CA Datacom/DB external security definitions.

Specific Resource Type Names

Resource type names in CA Top Secret match the generic names. Therefore the CA Datacom resources are DTSYSTEM, DTADMIN, DTTABLE, DXTABLE, DCTABLE, DFTABLE, DGTABLE, DHTABLE, DPTABLE, DQTABLE, DRTABLE, DSTABLE, and DTUTIL. When specifying these resources in an ADD statement, you can use up to 26 characters.

In CA Top Secret, the DTSYSTEM, DTADMIN, and DTUTIL resources include an access level. This is done only so that all CA Top Secret generic resource names are supported. You do not code access levels for these resources when specifying individual permissions.

Caution Limited Documentation

The following information is not intended to replace nor supersede any information in the CA Top Secret documentation for the version being executed. The samples are not intended to display all features of CA Top Secret. The specific rules provided in the DTUTIL and DTTABLE resource classes are examples and are not intended as guidelines for establishing a secured environment.

Adding a Facility

In the following steps, the MUF region ACID is assumed to be MUFPROD1 and the CA Datacom Facility name is PRODMUF1.

Step 1

To establish external security in CA Top Secret for the MUF, you must first create a Facility. Add the following statements to the Parameter File in CA Top Secret. The Facility name (PRODMUF1) represents this MUF. The *nn* and Facility name must be unique for each MUF.

```
FAC(USERnn=NAME=PRODMUF1)
```

Specify the Facility name (PRODMUF1) and specify *** to note that any CA Datacom/DB Multi-User program can interface with CA Top Secret.

```
FAC(PRODMUF1=PGM=***)
```

Specify the following options for the MUF. The defaults for other options provided by CA Top Secret should be acceptable.

```
FAC(PRODMUF1=MULTIUSER,AUTHINIT,RES,SHRPRF,NOABEND,SIGN(M))
```

Step 2

Once the Facility is set up, create a region ACID for the MUF using a CA Top Secret command similar to the following. There are other options which may be desirable. The department must already exist.

```
TSS CREATE(MUFPROD1) NAME('datacom-production-muf-1') DEPT(deptacid)
    FAC(BATCH,STC) PASS(NOPW)
```

Step 3

Relate the region ACID and the Facility:

```
TSS ADD(MUFPROD1) MASTFAC(PRODMUF1)
```

The MASTFAC parameter here associates the region ACID with the Facility entry made in the Parameter File. You could simply include the MASTFAC parameter in the CREATE statement which has the same effect as this step.

If a user other than MUFPROD1 runs the MUF as a batch job, a USER=MUFPROD1 parameter must be included in the job stream. To use the USER=MUFPROD1 option, the user must have authorization, such as TSS PER(userid) ACID(MUFPROD1).

Step 4

If you run the MUF as a started task, add it to the Started Task table in CA Top Secret:

```
TSS ADD(STC) PROC(procmuf1) ACID(MUFPROD1)
```

The PROC name (procmuf1) would be the name of the PROC that occurs in SYS1.PROCLIB.

Step 5

Any user who needs access to the MUF must be identified with the Facility:

```
TSS ADD(userid) FAC(PRODMUF1)
```

Step 6

At this point, CA Top Secret security has been properly established (assuming the CA Datacom RDTs have been defined by having current maintenance, or manually applied). All MUFs are at this time *not* secured. To secure any, some, or all MUFs, add one or more entries with the DTSYSTEM class. Do NOT secure your MUFs until you have built the desired DTADMIN, DTTABLE, and DTUTIL entries.

Sample Entries to Secure CA Datacom

Before permissions are added, the resource must be added. To enable security, add the DTSYSTEM resource for the Directory (CXX) name using the following format. This entry secures all products for this Directory.

```
TSS ADD(deptacid) DTSYSTEM(cxxname).
```

An enable of the MUF at this point causes it to be fully secured. To have any product unsecured from external security, add permissions to either all users, or at least the USERID for the MUF startup using the following format, where xx is DB, DD, or DQ:

```
TSS PER(userid) DTSYSTEM(cxxname.xx)
```

To unsecure multiple products, provide multiple statements.

Defining Access Rights of Users

At this point, all users have full access to define administrators. Enter the following to define an administrator and block all other users.

```
TSS ADD(deptacid) DTADMIN(PRODCXX.DB)
TSS PER(userid) DTADMIN(PRODCXX.DB)
```

Adding permissions to the other CA Datacom resource classes is more obvious. Here are some examples:

```
TSS ADD(deptacid) DTTABLE(PRODCXX.DB00001)
TSS ADD(deptacid) DTUTIL(PRODCXX.DBUTLTY)
TSS ADD(deptacid) DTUTIL(PRODCXX.DB00001)
TSS PER(userid) DTTABLE(PRODCXX.DB00001.PAY) ACCESS(READ)
TSS PER(userid) DTTABLE(PRODCXX.DB00001.PMF) ACCESS(ALL)
TSS PER(userid) DTTABLE(PRODCXX.DB00001.POH) ACCESS(NONE)
TSS PER(userid) DTUTIL(PRODCXX.DBUTLTY.BACKUP.DATA)
TSS PER(userid) DTUTIL(PRODCXX.DBUTLTY.LOAD.DATA)
TSS PER(userid) DTUTIL(PRODCXX.DB00001.PAY.BACKUP)
TSS PER(userid) DTUTIL(PRODCXX.DB00001.PAY.LOAD)
```

For more information, see Enabling Online Signons (see page 61).

Security Interfaces, CA Top Secret (z/VSE)

Supported Versions

CA Top Secret z/VSE Version 3.0 and later support CA Datacom/DB external security definitions. The resource definition for the CA Datacom resources was provided to CA Top Secret z/VSE Version 3.0.

Specific Resource Type Names

Resource type names in CA Top Secret match the generic names. Therefore, the CA Datacom resources are DTSYSTEM, DTADMIN, DTTABLE, DXTABLE, DCTABLE, DFTABLE, DRTABLE, DSTABLE, and DTUTIL. When specifying these resources in an ADD statement, you can use up to 26 characters.

In CA Top Secret, the DTSYSTEM, DTADMIN, and DTUTIL resources include an access level. This is done only so that all CA Top Secret generic resource names are supported. You do not code access levels for these resources when specifying individual permissions.

Caution Limited Documentation

The following information is not intended to replace nor supersede any information in the CA Top Secret documentation. The samples are not intended to display all features of CA Top Secret. Knowledge of CA Top Secret z/VSE security definitions is required. The specific rules provided in the DTUTIL and DTTABLE resource classes are examples and are not intended as guidelines for establishing a secured environment.

Adding a Facility

In the following steps, the MUF region ACID is assumed to be MUFPROD1 and the CA Datacom Facility name is PRODMUF1.

Step 1

To establish external security in CA Top Secret for the MUF, you must first create a Facility. To do this, add the following statements to the Parameter File in CA Top Secret. The Facility name (PRODMUF1) represents this MUF. The *nn* and Facility name must be unique for each MUF.

```
FAC(USERnn=NAME=PRODMUF1)
```

Specify the Facility name (PRODMUF1) and specify *** to note that any CA Datacom/DB Multi-User program may interface with CA Top Secret.

```
FAC(PRODMUF1=PGM=***)
```

Specify the following options for the MUF. The defaults for other options provided by CA Top Secret should be acceptable.

```
FAC(PRODMUF1=MULTIUSER,AUTHINIT,RES,SHRPRF,NOABEND,SIGN(M))
```

Step 2

Once the Facility is set up, create a region ACID for the MUF using a CA Top Secret command similar to the following. There are other options which may be desirable. The department must already exist.

```
TSS CREATE(MUFPROD1) NAME('datacom-production-muf-1')DEPT(deptacid)
  FAC(BATCH) PASS(NOPW)
```

Step 3

Relate the region ACID and the Facility:

```
TSS ADD(MUFPROD1) MASTFAC(PRODMUF1)
```

The MASTFAC parameter here associates the region ACID with the Facility entry made in the Parameter File. You could simply include the MASTFAC parameter in the CREATE statement which has the same effect as this step.

If a user other than MUFPROD1 runs the MUF as a batch job, a USER=MUFPROD1 parameter must be included in the job stream. To use the USER=MUFPROD1 option, the user must have authorization, such as TSS PER(userid) ACID(MUFPROD1).

Step 4

Any user who needs access to the MUF must be identified with the Facility:

```
TSS ADD(userid) FAC(PRODMUF1)
```

Step 5

At this point, CA Top Secret security has been properly established assuming that the CA Datacom RDTs have been defined by having current maintenance, or manually applied. All MUF are at this time *not* secured. To secure any, some, or all MUF, add one or more entries with the DTSYSTEM class. Do *not* secure your MUF until you have built the desired DTADMIN, DTTABLE, and DTUTIL entries.

Defining Access Rights of Users

At this point, all users have full access to define administrators. Enter the following to define an administrator and block all other users.

```
TSS ADD(deptacid) DTADMIN(PRODCXX.DB)
TSS PER(userid) DTADMIN(PRODCXX.DB)
```

Adding permissions to the other CA Datacom resource classes is more obvious. Here are some examples:

```
TSS ADD(deptacid) DTTABLE(PRODCXX.DB00001)
TSS ADD(deptacid) DTUTIL(PRODCXX.DBUTLTY)
TSS ADD(deptacid) DTUTIL(PRODCXX.DB00001)
TSS PER(userid) DTTABLE(PRODCXX.DB00001.PAY) ACCESS(READ)
TSS PER(userid) DTTABLE(PRODCXX.DB00001.PMF) ACCESS(ALL)
TSS PER(userid) DTTABLE(PRODCXX.DB00001.POH) ACCESS(NONE)
TSS PER(userid) DTUTIL(PRODCXX.DBUTLTY.BACKUP.DATA)
TSS PER(userid) DTUTIL(PRODCXX.DBUTLTY.LOAD.DATA)
TSS PER(userid) DTUTIL(PRODCXX.DB00001.PAY.BACKUP)
TSS PER(userid) DTUTIL(PRODCXX.DB00001.PAY.LOAD)
```

For more information, see Enabling Online Signons (see page 61).

Security Interfaces, RACF

Limited Documentation

The following information is not intended to replace nor supersede any information in the RACF documentation for the version being executed. Any samples are not intended to display all features of RACF.

The IBM RACF facility for a z/OS environment supports user-defined resources which can be used by CA Datacom. Changes are required to the CAISSF component of CA Common Services for z/OS. See the *CA Common Services for z/OS Installation Guide*.

Note: To help ensure proper CICS interface with the IBM RACF product, verify that the DFHSIT macro parameter EXTSEC is coded YES. We also recommend coding the IBM DFHSNT macro parameter EXTSEC=YES. For more information, see IBM documentation.

User resource names in RACF are required to have a special character in the name. The CA Datacom resource names are altered for RACF as follows. The pattern is that the third character in the resource name is replaced with an @ sign.

CA Datacom/DB	RACF
DTSYSTEM	DT@YSTEM
DTADMIN	DT@DMIN
DTTABLE	DT@ABLE
DXTABLE	DX@ABLE
DCTABLE	DC@ABLE
DFTABLE	DF@ABLE
DRTABLE	DR@ABLE
DSTABLE	DS@ABLE
DGTABLE	DG@ABLE
DHTABLE	DH@ABLE
DPTABLE	DP@ABLE
DQTABLE	DQ@ABLE
DTUTIL	DT@TIL

Add the resource name definitions (from the previous table) to the RACF Class Descriptor table (ICHERCDE) and to the RACF SAF Router Table (ICHRFRTB). See your RACF documentation for the syntax for these commands.

The RACF resource rights (arranged in hierarchical sequence) for the DTTABLE resource class equate to those for CA Datacom/DB as follows:

CA Datacom/DB	RACF
READ	READ
UPDATE	UPDATE
DELETE	CONTROL
ADD	ALTER

RACF authorizations are hierarchical, that is:

- READ authority allows only read access.
- UPDATE authority allows read and update access.
- CONTROL authority allows read, update, and delete access.
- ALTER authority allows read, update, delete, and add access.

Add the specific security rules to secure the CA Datacom resources as defined in the general documentation section earlier in this chapter.

For more information, see Enabling Online Signons (see page 61).

Refreshing RACF Without Cycling Multi-User

A problem reported by customers when updating RACF resources that are used with CA Datacom/DB external security is that the RACF environment is not automatically refreshed unless the MUF (MUF) is recycled. The following option provides a method to refresh the RACLIST and allows you to incorporate security file changes into an active MUF instead of forcing you to recycle.

Change Resource Translation Table

Beginning with CA Common Services (CCS) Version 14.1, changes to the CAS9SAFC resource translation table entries are performed using a new enhanced method. It is done using a CAS9 startup data set identified by a //CAIRACF DD statement instead of having to change, assemble and link edit the CCS CAS9SAFC source module. The data set can be a sequential data set or a PDS. In either case the LRECL must be 80. The appropriate overrides for the CA Datacom core product components are located in the SMP/E CABDSAMP library member CAS9SAFC. The CABDSAMP CAS9SAFC member can either be reference directly in the CCS CAS9 startup JCL or copied to a different data set.

For more information see the Version 14.1 *CA Common Services Administration Guide*. The following sample CAS9 startup JCL CAIRACF DD statement shows the direct reference method.

```
//CAIRACF  DD  DISP=SHR,DSN=CAI.SHLQ.CABDSAMP(CAS9SAFC)
```

The CAI.SHLQ.CABDSAMP(CAS9SAFC) member contents are as follows:

```
RACFCLASS DTSYSTEM,DT@YSTEM,FASTAUTH=NO,CICS=YES
RACFCLASS DTADMIN,DT@DMIN,FASTAUTH=NO,CICS=YES
RACFCLASS DTUTIL,DT@TIL,FASTAUTH=NO,CICS=YES
RACFCLASS DTTABLE,DT@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DGTABLE,DG@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DXTABLE,DX@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DCTABLE,DC@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DFTABLE,DF@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DRTABLE,DR@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DSTABLE,DS@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DGTABLE,DG@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DHTABLE,DH@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DPTABLE,DP@ABLE,FASTAUTH=NO,CICS=YES
RACFCLASS DQTABLE,DQ@ABLE,FASTAUTH=NO,CICS=YES
```

For CA Common Services (CCS) Versions prior to 14.1, change the resource translation table in the CCS provided CAS9SAFC source member to indicate that a RACCHECK rather than FRACCHECK should be issued.

The following steps describe the necessary changes to the CAS9SAFC source for this option:

1. Edit the CAS9SAFC member in the CAISRC library
2. Locate the CAREPORT row in the resource translation table. Change the fourth column from '80' to '00' (x'80' says a FRACHECK is issued, and x'00' says a RACHECK is issued)

3. Add the following entries in the CAS9SAFC member based on the level of security you are defining:

   For Security Level 1, the DC Statement is as follows:

   ```
   C'DTSYSTEM',C'DT@YSTEM',X'00',X'00',X'00',X'00'
   C'DTADMIN ',C'DT@DMIN ',X'00',X'00',X'00',X'00'
   C'DTUTIL  ',C'DT@TIL  ',X'00',X'00',X'00',X'00'
   C'DTTABLE ',C'DT@ABLE ',X'00',X'00',X'00',X'00'
   ```

   For Security Level 2 the DC Statement is the same as for Level1, plus the following:

   ```
   C'DXTABLE ',C'DX@ABLE ',X'00',X'00',X'00',X'00'
   ```

   For Security Level 3 the DC Statement is the same as for Level1, and Level2, plus the following:

   ```
   C'DCTABLE ',C'DC@ABLE ',X'00',X'00',X'00',X'00'
   C'DFTABLE ',C'DF@ABLE ',X'00',X'00',X'00',X'00'
   C'DRTABLE ',C'DR@ABLE ',X'00',X'00',X'00',X'00'
   C'DSTABLE ',C'DS@ABLE ',X'00',X'00',X'00',X'00'
   ```

   For Security Level 4 the DC Statement is the same as for Level3.

   For Security Level 5 the DC Statement is the same as for Level1, Level2, and Level3, plus the following:

   ```
   C'DGTABLE ',C'DG@ABLE ',X'00',X'00',X'00',X'00'
   C'DHTABLE ',C'DH@ABLE ',X'00',X'00',X'00',X'00'
   C'DPTABLE ',C'DP@ABLE ',X'00',X'00',X'00',X'00'
   C'DQTABLE ',C'DQ@ABLE ',X'00',X'00',X'00',X'00'
   ```

4. After these changes are made, perform the following steps:

   a. A RACF online REFRESH and a SETROPTS REFRESH

   b. A DBUTLTY SECURITY RESET.

This option requires a reassembly of the CAS9SAFC module. The standard that CA uses is to apply a USERMOD named CAS9MOD which has a ++MOD for CAS9SAFC. The CA Common Services for z/OS installation guide documents this process under the section on Customizing CAISSF for RACF or RACF-Compatible Products. Member CAS9CSSF documented in the *CA Common Services for z/OS Installation Guide* contains the code for the RECEIVE and APPLY. With each maintenance cycle for CAIRIM, restore CAS9MOD before the maintenance APPLY and then reimplement the source changes before reapplying the USERMOD.

Chapter 3: DD Internal Security

This section discusses CA Datacom Datadictionary internal security. Securing CA Datacom Datadictionary using external security is discussed in Using External Security for CA Datacom.

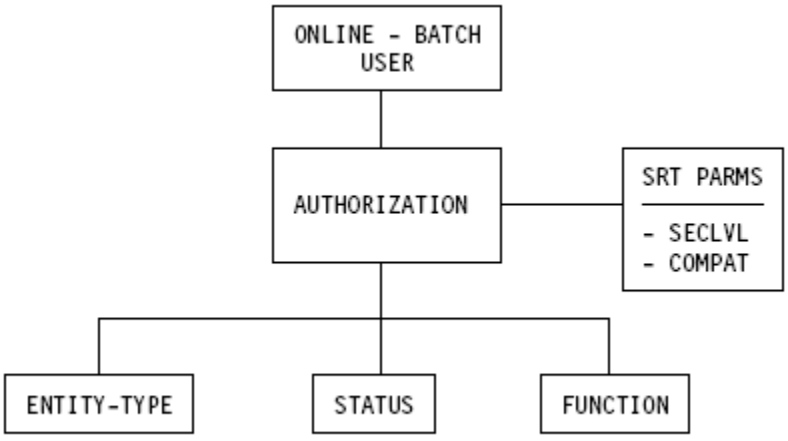
Securing CA Datacom Datadictionary Resources

The purpose of CA Datacom Datadictionary Security is to restrict access to CA Datacom Datadictionary resources to prevent unauthorized use. You can secure CA Datacom Datadictionary resources in several ways including levels of authority assigned to users and restrictions assigned to entity-occurrences.

Note: For more information about restricting access to entity-occurrences with passwords and lock levels, see the *CA Datacom Datadictionary User Guide*.

CA Datacom Datadictionary resources include:

- Batch and online facilities
- Entity-types
- Entity-types in a specific status
- Functions that can be performed on a specific entity-type in a specific status



CA Datacom Datadictionary Security is based on the following basic premises:

- Not every shop wants or needs the same level of security.

  The CA Datacom Datadictionary Security Facility allows you to determine the level of security required for your environment. The level of security is accomplished through a security level parameter in the System Resource Table (SRT).

  Note: For more information, see CA Datacom Datadictionary Security Model (see page 90) and the *CA Datacom/DB Database and System Administration Guide*.

  The following are examples of security level decisions:

  Small Shop

  Few people need access to CA Datacom Datadictionary and perform all functions. The only security necessary is PERSON entity-type level.

  Medium Shop

  Few people actually update CA Datacom Datadictionary, but many need access to the data. Restrict access to facilities which perform the updates.

  Large Shop

  Several projects are ongoing in different stages with different project teams. Restrict types of access to certain entity-types in given statuses.

- In most shops, groups of people require the same resource access. Therefore, rather than individually defining access, the concept of profiles was designed. Profiles are a definition of access levels used by groups of people. Profiles are defined and are connected or associated to PERSON entity-occurrence definitions.

If you have more than one CA Datacom Datadictionary, you can have different authorization levels in the different CA Datacom Datadictionary databases.

CA Datacom Datadictionary Security Features

The CA Datacom Datadictionary Security Facility provides the following:

- Five levels of CA Datacom Datadictionary Security
- Online and batch maintenance capabilities
- Implementation based on generalized profiles

Security Level

Security level is defined on a systemwide basis and defines the ultimate level of security needed at your site. It is determined by the SECLVL= parameter in the System Resource Table as defined in CA Datacom Datadictionary Security Model (see page 90). We recommend limited access to the System Resource Table macro.

In addition, you can use passwords and locks to restrict functions that can be performed on an entity-occurrence definition. If you assign a password to a definition, this password must be specified before performing maintenance on the definition.

Use locks to deny maintenance or access of any kind to the entity-occurrence definition. If you assign a lock, specify the correct override code for your site to perform any maintenance or gain access to the definition.

Note: For more information about using passwords and locks, see the *CA Datacom Datadictionary User Guide*.

Online Panels

CA Datacom Datadictionary online provides a series of panels for you to select menu items and enter data. These panels are accessed through the AUTHORIZE Mode (option 4 on the CA Datacom Datadictionary Mode Selection panel).

Batch Transactions

The batch facility provides transactions to use DDUPDATE utility to maintain PERSON entity-occurrences and profiles (AUTHORIZATION entity-occurrences) and DDCFBLD to catalog profiles to the CA Datacom Datadictionary High-Speed Directory (HSD).

Note: For more information about running DDUPDATE and DDCFBLD, see the *CA Datacom Datadictionary Batch Reference Guide*.

Profiles

Profiles define a set of access rules which can be assigned to one or more specific users. You establish profiles with the AUTHORIZATION entity-type. For example, you can establish your security system so that Database Administrators have full update access to all entity-types in the CA Datacom/DB Model, whereas systems analysts have only display access to DATABASE, AREA, and TABLE entity-types, but have update access to FIELD entity-types.

CA Datacom Datadictionary Security Model

The CA Datacom Datadictionary Security Facility is composed of the following components:

- Security level (SRT)
- People (PERSON)
- Profile (AUTHORIZATION entity-occurrence)
- Facilities (SYSTEM)
- Entity-Types (TABLE)
- Status
- Function
- Relationships

Security Level (SRT)

The level of security is site-dependent and is defined in the System Resource Table (SRT) parameter, SECLVL=. This parameter determines the level of security enforced by CA Datacom Datadictionary. If more security information is defined in a profile than is specified with the SECLVL= parameter, the information is used by the CA Datacom Datadictionary Security Facility, as appropriate.

Person Level SECLVL=0

Any user identified with a PERSON entity-occurrence is authorized access to most CA Datacom Datadictionary capabilities. An example is one or two people in a small shop.

Facility Level SECLVL=1

Restricts a user to selected batch and online facilities such as the DDUPDATE and DDCFBLD of batch or the CA File Maintenance Mode of CA Datacom Datadictionary online, and so on.

Entity Level SECLVL=2

Restricts access of a user to selected entity-types. For example, in a medium-sized shop, a group of people maintain, report, and develop definitions in CA Datacom Datadictionary and need full access in all statuses, while operation analysts need access to jobs, steps, and programs and do *not* need access to other definitions in CA Datacom Datadictionary.

Status Level SECLVL=3

Restricts access of a user to selected entity-types in a certain status. For example, developers designing files and databases change TEST status definitions and do not need to access PROD status definitions, while support personnel need access to PROD status definitions and do not need access to TEST status definitions.

Function Level SECLVL=4

Restricts access of a user to selected functions that can be performed on a certain entity-type in a certain status. For example, development personnel can retrieve, display, and update an entity-type in TEST status and only display PROD status definitions, while support personnel would have display-only access to TEST status and have retrieve, display, and update access to PROD status definitions.

Security levels are cumulative. In other words, Status Level security implies that Person Level security and Entity Level security have been defined.

Regardless of the level of security you choose, each person who is authorized to use CA Datacom Datadictionary must be defined with a PERSON entity-occurrence. Use either the batch or online security maintenance facilities to define PERSON entity-occurrences.

Profiles

Profiles are occurrences in the AUTHORIZATION entity-type and begin with $DD-. At the installation of CA Datacom Datadictionary Security, five profiles are predefined:

- $DD-ADM
- $DD-COP
- $DD-UPD
- $DD-DIS
- $DD-SEC-ADM

The first four profiles are provided for compatibility with previous CA Datacom Datadictionary versions. These profiles provide the same functional levels of security available in previous versions. $DD-SEC-ADM is a special profile used to define the Security Administrator authority. For more information, see Profiles Provided with CA Datacom Datadictionary Security (see page 103).

The PERSON entity-occurrences defined as having Security Administrator authority can use online and batch facilities. In addition, through security level 2 (SECLVL=0 - 2), *no one* has update authority against PROD status entity-occurrences unless specifically assigned that authority on an exception basis.

Other than the $DD-SEC-ADM profile, a profile (AUTHORIZATION entity-occurrence) alone is meaningless. It has to be related to facilities (SYSTEM entity-occurrences or entity-types (TABLE entity-occurrences) for security authorization to be enforced.

The Security Administrator defines and maintains profiles using either the batch or online maintenance facilities.

Facilities

You only need to define facilities if you have defined a security level of 1 or higher in the System Resource Table, SECLVL= parameter. Facilities are divided into two categories, online and batch. Each facility is represented by an entity-occurrence in the SYSTEM entity-type. These entity-occurrences are provided by CA Datacom Datadictionary when the product is installed and should not be modified or deleted. They can be recognized by their entity-occurrence name which begins with $DD-. The facilities secured by CA Datacom Datadictionary Security are:

ID	Batch Facility
BTG	DDBTGLM maintenance
CFB	DDCFBLD maintenance
RMF	DDRMFLM maintenance
TRS	DDTRSLM maintenance
UPD	DDUPDATE maintenance
UTL	DDUTILTY maintenance

The Source Language Generation function is accessed through the DDUTILTY utility and is therefore secured when you secure the utility. The CA Datacom Datadictionary Input Creation Facility (DDICF) is *not* secured since it does not access CA Datacom Datadictionary directly and security must be invoked to execute the transactions generated.

Note: For more information about the CA Datacom Datadictionary utilities, see the *CA Datacom Datadictionary Batch Reference Guide*.

ID	Online Facility
DBM	CA Datacom/DB Structure Maintenance

ENTD	CA Datacom Datadictionary Entity Display
ENTM	CA Datacom Datadictionary Entity Maintenance
FMM	File Structure Maintenance
ISF	Interactive Service Facility
SQL	Interactive SQL Service Facility

Note: For more information about using the online facilities, see the *CA Datacom Datadictionary Online Reference Guide*.

Entity-Types (TABLES)

You only need to define entity-types if you have defined a security level of 2 or higher in the System Resource Table, SECLVL= parameter. Entity-types are represented in CA Datacom Datadictionary by TABLE entity-occurrences with a DD-ENTY-TYPE attribute-value of Y. The following can be secured with CA Datacom Datadictionary product security:

AREA
AUTHORIZATION
CONSTRAINT
DATABASE
DATAVIEW
ELEMENT
FIELD
FILE
JOB
KEY
LIBRARY
MEMBER
MODULE
NODE
PANEL
PARAMETER-LIST
PARTITION-COLUMN-VALUE
PARTITION-VALUE
PERSON
PLAN
PROCEDURE
PROGRAM
RECORD
RELATIONSHIP
REPORT
STATEMENT
STEP
SYNONYM
SYSTEM
TABLE
TRIGGER
UNIVERSAL (record)
VIEW

Note: Although aliases, descriptors, and text are also represented by TABLE entity-occurrences, use security level 4 to limit their use.

Status

If you have defined a security level of 3 or higher in the System Resource Table SECLVL= parameter, you can limit access to an entity-occurrence within an entity-type by status. This is represented in CA Datacom Datadictionary by a special relationship between the profile (AUTHORIZATION entity-occurrence) and the entity-type (TABLE).

The relationship name indicates the status of the entity-occurrence to which the profile authorizes access. The relationship is defined by CA Datacom Datadictionary as $DD-ATZ-ENT-x, where x is the status of the entity-occurrence to which the profile authorizes access. P indicates PROD status, T indicates a generic TEST status, 001—999 indicates a specific TEST status, and SEC is for all statuses. The CA Datacom Datadictionary Security Facility defines these special relationships automatically as needed. For more information, see Relationships (see page 100).

Function

For security level 4, in addition to defining all previous access rights, you can further limit access of a user to entity-occurrences of a particular entity-type by limiting the functions that can be applied to the entity-occurrence of that particular entity-type in a particular status.

The functions that you can define are shown in the following chart. The code is the abbreviation that appears on the Security Profile maintenance panels.

Function		Code Description
ALIAS maintenance	ALS	Maintain ALIAS information for a given entity-type.
ADD/CREATE	ADD	Add or create entity-occurrences using batch or online maintenance facilities, or add entity-occurrences to user-defined entity-types using CA Datacom Datadictionary Service Facility.
CATALOG	CAT	Perform the CATALOG function using either batch or online maintenance facilities.
COPY from	FRM	Copy an entity-occurrence *from* the specified status.

Function		Code Description
COPY to	TO	Copy an entity-occurrence *to* the specified status. That is, the user is authorized to copy DATABASE structure from T001 status to PROD status, and not *to* or *from* any other status.
DEFINE	DEF	Maintain FIELD entity-occurrences within TABLE, RECORD, KEY, and ELEMENT entity-occurrences. Also maintain universal field definitions using this function. **Note:** The universal field facility allows you to define a field once, and to define multiple record definitions.
DELETE/REMOVE	DEL	Delete entity-occurrence using batch or online maintenance facilities or delete entity-occurrence from user-defined entity-types using CA Datacom Datadictionary Service Facility.
DESCRIPTOR maintenance	DES	Maintain DESCRIPTOR information for a given entity-type.
DISPLAY/RETRIEVE	DIS	Display entity-occurrence information using batch or online facilities. Retrieve entity-occurrence information using CA Datacom Datadictionary Service Facility.
DISABLE	DSA	Perform the DISABLE function using either batch or online maintenance facilities.
ENABLE	ENA	Perform the ENABLE function using either batch or online maintenance facilities.
OBSOLETE	OBS	Perform the OBSOLETE function using either batch or online maintenance facilities. This function applies to *all* statuses of the CA Datacom/DB and CA FILE Model Structures and can therefore *only* be specified for the ALL (SEC) level.
PASSWORD/LOCK maintenance	SEC	Maintain password and lock level information for a given entity-occurrence.

Function		Code Description
RELATE/TRANSFER maintenance	REL	Add, update, delete, modify relationships between two entity-types or for a relationship defined between the same entity-type. To maintain these relationships, you must be authorized RELATIONSHIP maintenance access for both the subject and object entity-types. Additionally, if you are authorized this access to AREA, TABLE, FILE, and RECORD entity-types, you can perform the TRANSFER function in either online or batch.
RESTORE	RES	Restore an entity-occurrence or structure to the specified status from either PROD status or HIST status.
SET	SET	Perform the SET function using either batch or online maintenance facilities. SET is a valid function for the DATABASE entity-type only.
STATUS maintenance	STA	Change the status of entity-occurrences using either online or batch facilities. This function only applies to entity-types other than DATABASE, AREA, FILE, RECORD, TABLE, VIEW, SYNONYM, FIELD, KEY, ELEMENT, and DATAVIEW.
TEXT maintenance	TXT	Maintain TEXT information for a given entity-type.
UPDATE/MODIFY	UPD	Update or modify entity-occurrences (including entity-occurrence names, the RENAME function) using batch or online maintenance facilities or update entity-occurrences from user-defined entity-types using CA Datacom Datadictionary Service Facility.
VERIFY	VER	Perform the VERIFY function using either batch or online maintenance facilities.

There are several rules to understand at this level of security:

- Relative to a structure, a DELETE or a COPY implies that the function is available for the entire structure or substructure, but only at the level implied by the related entity-type.

  For example, if DELETE is specified for the TABLE entity-type, that function can be performed for the TABLE substructure without having to define DELETE for the KEY and ELEMENT levels. However, you cannot perform the DELETE function at the KEY or ELEMENT level unless you are specifically authorized to use this function.

- Authorization for any function implies DISPLAY/RETRIEVE authority.
- MODEL is not specifically secured. If a user is authorized to perform ADD or CREATE, they can use modeling.
- Function information is maintained by the CA Datacom Datadictionary Security Facility in the intersection data of the relationship between the profile (AUTHORIZATION entity-occurrence) and the entity-type (TABLE).

Valid Entity-Type and Function Combinations

The following chart shows the valid combination of entity-types, status, and functions that can be used in CA Datacom Datadictionary. Most invalid function and entity-type combinations are ignored. For example, CA Datacom Datadictionary does not prevent you from assigning the SET function to the PROGRAM entity-type, but CA Datacom Datadictionary would not select it because SET is not a valid function for a PROGRAM entity-occurrence.

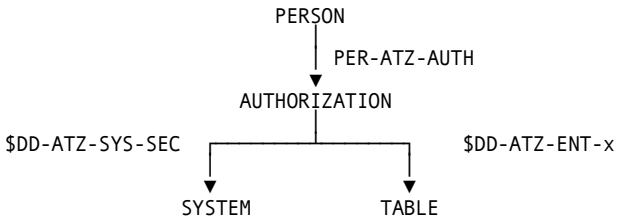
Entity-Type	Status	Valid Functions
ALIAS	PROD TEST	ADD, DEL, DIS, UPD
AREA	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, REL, TO, TXT, UPD
AUTHORIZATION	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
CONSTRAINT	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
DATABASE	PROD TEST T001—T999	ADD, ALS, CAT, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, SET, TO, TXT, UPD, VER
DATAVIEW	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, TO, TXT, UPD

Entity-Type	Status	Valid Functions
DESCRIPTOR	PROD TEST	ADD, DEL, DIS, UPD
ELEMENT	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, TO, TXT, UPD
FIELD	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
FILE	PROD TEST T001—T999	ADD, ALS, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, TO, TXT, UPD, VER
JOB	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
KEY	PROD TEST T001—T999	ADD, ALS, DEF, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, TO, TXT, UPD
LIBRARY	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
MEMBER	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
MODULE	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
NODE	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PANEL	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PARAMETER-LIST	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
PARTITION-COLUMN-VALUE	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PARTITION-VALUE	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PERSON	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
PLAN	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD

Entity-Type	Status	Valid Functions
PROCEDURE	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
PROGRAM	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
RECORD	PROD TEST T001—T999	ADD, ALS, DEF, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, TO, TXT, UPD
RELATIONSHIP	PROD TEST	ADD, DEL, DIS, UPD
REPORT	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
STATEMENT	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
STEP	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
SYNONYM	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
SYSTEM	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
TABLE	PROD TEST T001—T999	ADD, ALS, DEF, DEL, DES, DIS, FRM, DSA, ENA, OBS, REL, RES, SET, TO, TXT, UPD
TEXT	PROD TEST	ADD, DEL, DIS, UPD
TRIGGER	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD
UNIVERSAL (record)	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
user-defined entity-type	PROD TEST	ADD, ALS, DEL, DES, DIS, FRM, REL, TO, TXT, UPD
VIEW	PROD TEST	ALS, DEL, DES, DIS, SEC, TXT, UPD

Relationships

In CA Datacom Datadictionary, models are made up of entity-types and defined relationships. The entity-types and relationships in the CA Datacom Datadictionary Security model are:



In defining a profile (AUTHORIZATION entity-occurrence), the entity-occurrence is not meaningful until it is related to the facilities (represented by the SYSTEM entity-occurrences) and the entity-types (represented by TABLE entity-occurrences).

The relationships used are either predefined and are present at installation, or the definitions are generated by the CA Datacom Datadictionary Security Facility as required.

- Profile/Facilities Relationship (SYSTEM) - Are predefined at installation and are defined as $DD-ATZ-SYS-SEC. The relationship indicates that this profile authorizes access to the facility represented by the SYSTEM entity-occurrence.
- Profile/Entity-Type Relationship (TABLE) - Are not predefined at installation other than $DD-ATZ-ENT-SEC which is used to specify access to all statuses of an entity-type.

  To define what entity-types are available for a profile, the status and function must also be defined. Status is defined through the actual relationship name. For example, the relationship $DD-ATZ-ENT-SEC is predefined and authorizes access to *all* statuses.

  Other relationships are defined by CA Datacom Datadictionary as the profiles are defined. For example, $DD-ATZ-ENT-001 authorizes access to entity-occurrences in T001 status.

  Functions are tied to profile, entity-type, and status. This data becomes part of the profile to entity-type relationship with Intersection Data. It is retained by CA Datacom Datadictionary in the form of 1-byte flags which represent the functions allowed against the entity-types in a defined status.
- Person/Authorization Relationship - Is used not only by CA Datacom Datadictionary, but by other CA products such as CA Ideal, and is defined as PER-ATZ-AUTH. For CA Datacom Datadictionary Security, this relationship defines the profile to which a PERSON entity-occurrence is assigned.

CA Datacom Datadictionary Security Authorization Process

The following explains the validation process used in the CA Datacom Datadictionary Security Facility to enforce the implemented security.

Person Authorization

If SECLVL=0, the Security Facility checks for a PERSON entity-occurrence in PROD status. The check is made when:

- The -USR transaction is processed in a batch utility.
- The CA Datacom Datadictionary signon panel is processed.
- The SET DBID command is processed in online CA Datacom Datadictionary.
- When a USRINITI CA Datacom Datadictionary Service Facility command is processed.
- When a SET USER command is processed in DDTRSLM.

At this minimum level of security, no other checks are required except for access to the Security Facilities, but update access to PROD status entity-occurrences can be defined and are allowed. To access the Security Facilities at least one user must be authorized as the CA Datacom Datadictionary Security Administrator, as defined next.

Profile Authorization

If SECLVL is greater than 0, the Security Facility checks to see that the PERSON entity-occurrence is related to at least one and no more than two AUTHORIZATION entity-occurrences beginning with $DD-.

If there are two, one of them *must* be $DD-SEC-ADM. This is a special authorization for the CA Datacom Datadictionary Security Administrator. The $DD-SEC-ADM AUTHORIZATION entity-occurrence cannot be deleted or modified and must always be related to at least one PERSON entity-occurrence.

All other AUTHORIZATION entity-occurrences beginning with $DD- are user-defined, with the exception of $DD-ADM, $DD-COP, $DD-UPD, and $DD-DIS. These are maintained for compatibility with earlier versions.

AUTHORIZATION entity-occurrences are related to one or more special SYSTEM entity-occurrences or one or more TABLE entity-occurrences in PROD status with a DD-ENTITY-TABLE attribute-value of Y. These relationships determine what facilities the user is authorized to use and which entity-types can be accessed. In addition, for the entity-types, the functions that can be performed and the statuses accessible are defined by these relationships.

Note: The CA Datacom Datadictionary Security Facility *does not* read all of this information at execution time. It reads the condensed information from the CA Datacom Datadictionary High-Speed Directory (HSD). This HSD member is the "cataloged" profile.

Facility Authorization

If SECLVL=1, the Security Facility checks for the AUTHORIZATION entity-occurrence to which the PERSON entity-occurrence is related. It also checks for a relationship to one or more special SYSTEM entity-occurrences. SYSTEM entity-occurrence names can be batch or online. For a description of the valid batch and online facility values, see Facilities (see page 92).

Entity Authorization

If SECLVL=2, the system checks for the AUTHORIZATION entity-occurrence to PERSON entity-occurrence relationship and for the related TABLE entity-occurrence(s) representing the entity-types to which the user has access. User access to given entity-types is authorized by the relationship between an AUTHORIZATION entity-occurrence and the TABLE entity-occurrence.

Status Authorization

If SECLVL=3, the system checks for the relationships in the Facility and Entity Authorization steps previously described. In addition, it checks for authorization to a given entity-type in a given status. The STATUS authorizations can be in ALL, PROD, HIST, TEST, or a specific version (T001—T999) can be indicated. Occurrences in HIST status are checked only when the DELETE function is issued. If the security level (SECLVL= parameter) is 0, 1, or 2, maintenance access to PROD status entity-occurrences and the DELETE function accepted for HIST status entity-occurrences can be defined as with other levels and is allowed. Otherwise, no user at these levels has maintenance authority for entity-occurrences in PROD status or HIST status.

Function Authorization

If SECLVL=4, the system checks for the relationships in the Facility, Entity, and Status Authorization steps previously described. In addition, it checks for authorization to perform certain functions to the previously defined entity-types.

Profiles Provided with CA Datacom Datadictionary Security

The following section documents standard profiles provided with CA Datacom Datadictionary. These profiles can be modified, if necessary.

$DD-SEC-ADM Profile (Security Administrator)

Only the $DD-SEC-ADM profile is defined with Security Administrator privileges. No other privileges are associated with this profile. It is the only profile that can be assigned to a person coincidentally with a second profile. Additionally, there must be at least one person with this profile. It is the only profile without a coinciding occurrence in the AUTHORIZATION entity-type.

Predefined Profiles

The following information describes the access allowed by each of the four predefined profiles. The columns indicate the access allowed for each Profile based on the security level (specified with the DDSYSTBL macro parameter SECLVL=) chosen to be enforced.

These Profiles allow the indicated privileges for the entity-types that are included in the standard installation of CA Datacom Datadictionary. For more information, see Valid Entity-Type and Function Combinations (see page 48). The following codes are used in the matrix:

Code	Security Level
F	Facilities
E	Entities
P	Functions (Privilege to perform Functions)
MNT	All maintenance functions. For example, MNT TEST indicates that a user with the indicated Profile can perform all maintenance functions against entity-occurrence in TEST status.

$DD-ADM Profile

```
PERSON     FACILITY    ENTITY-TYPE   STATUS      FUNCTIONS

SECLVL=0   SECLVL=1    SECLVL=2      SECLVL=3    SECLVL=4
_____________________________________________________________________________
F=ALL       F=ALL       F=ALL         F=ALL       F=ALL
E=ALL       E=ALL       E=ALL         E=ALL       E=ALL
P=ALL       P=ALL       P=ALL         P=ALL       P=ALL (except OBSOLETE)
```

$DD-COP Profile

```
  PERSON     FACILITY    ENTITY-TYPE   STATUS      FUNCTIONS
_____________________________________________________________________________
  SECLVL=0   SECLVL=1    SECLVL=2      SECLVL=3    SECLVL=4
  F=ALL      F=DDUTILTY  F=DDUTILTY    F=DDUTILTY  F=DDUTILTY
               DDUPDATE    DDUPDATE      DDUPDATE    DDUPDATE
               ENTDISPL    ENTDISPL      ENTDISPL    ENTDISPL
               ENTMAINT    ENTMAINT      ENTMAINT    ENTMAINT
               DBMAINT     DBMAINT       DBMAINT     DBMAINT
               FILEMAINT   FILEMAINT     FILEMAINT   FILEMAINT
  E=ALL      E=ALL       E=ALL         E=ALL       E=ALL
  P=DIS ALL  P=DIS ALL   P=DIS ALL     P=DIS ALL   P=DIS, ADD, DEL , UPD, TXT
    MNT TEST   MNT TEST    MNT TEST      MNT TEST    REL, SET, VER, ALS, DES,
                                                       FLD in TEST status
                                                       DIS ALL
```

$DD-DIS Profile

```
PERSON     FACILITY      ENTITY-TYPE   STATUS       FUNCTIONS

SECLVL=0   SECLVL=1      SECLVL=2      SECLVL=3     SECLVL=4
F=ALL      F=DDUTILTY    F=DDUTILTY    F=DDUTILTY   F=DDUTILTY
             ENTDISPL      ENTDISPL      ENTDISPL     ENTDISPL
E=ALL      E=ALL         E=ALL         E=ALL        E=ALL
P=DIS ALL  P=DIS ALL     P=DIS ALL     P=DIS ALL    P=DIS ALL
  MNT TEST
```

Exception:

This profile does not allow display of the entity-types used for SQL processing (CONSTRAINT, PLAN, STATEMENT, SYNONYM, and VIEW).

$DD-UPD Profile

```
PERSON      FACILITY      ENTITY-TYPE    STATUS       FUNCTIONS

SECLVL=0    SECLVL=1      SECLVL=2       SECLVL=3     SECLVL=4
F=ALL       F=DDUTILTY    F=DDUTILTY     F=DDUTILTY   F=DDUTILTY
              DDUPDATE      DDUPDATE       DDUPDATE     DDUPDATE
              ENTDISPL      ENTDISPL       ENTDISPL     ENTDISPL
              ENTMAINT      ENTMAINT       ENTMAINT     ENTMAINT
              DBMAINT       DBMAINT        DBMAINT      DBMAINT
              FILEMAINT     FILEMAINT      FILEMAIN     FILEMAINT
E=ALL       E=ALL         E=ALL          E=ALL        E=ALL
P=DIS ALL   P=DIS ALL     P=DIS ALL      P=DIS ALL    P=DIS, ADD, DEL, UPD, TXT
  MNT TEST    MNT TEST      MNT TEST       MNT TEST     REL, SET, VER, ALS, DES,
                                                        FLD in TEST status
                                                        DIS ALL
```

User-Defined Profiles Examples

The following matrix describes examples of possible profiles and the effect of the security levels on the profile.

The first column of the matrix lists the privileges assigned to the profile by entity-type and status. The remaining columns indicate the access allowed for each Profile based on the security level (SECLVL=) chosen to be enforced.

In the matrix, the term MNT PROD JOB, RPT indicates that the user could perform maintenance functions against entity-occurrences of the JOB and REPORT entity-types in PROD status. All other codes are the same as in the previous matrixes.

Example: $DD-USER1

Privileges	PERSON	FACILITY	ENTITY-TYPE	STATUS	FUNCTIONS
Assigned	SECLVL=0	SECLVL=1	SECLVL=2	SECLVL=3	SECLVL=4
F=DDUPDATE ENTD FMM	F=ALL	F=DEF	F=DEF	F=DEF	F=DEF
E=RPT (ALL)	E=ALL	E=ALL	E=RPT, JOB, SYS	E=RPT,JOB, SYS	E=RPT, JOB, SYS
P=ADD, DISP DEL	P=DIS ALL MNT TEST MNT PROD JOB, RPT	P=DIS ALL MNT TEST MNT PROD JOB, RPT	P=DIS RPT, JOB, SYS MNT TEST RPT, JOB, SYS MNT PROD JOB, RPT	P=DIS RPT, JOB, SYS MNT ALL RPT MNT PROD JOB MNT TEST SYS DEL, TEST SYS	P=DIS, ADD, DEL ALL RPT DIS, UPD ALL PROD JOBS ADD, DISP, UPD,
E=JOB (PROD) P=DIS, UPD					
E=SYS (TEST) P=ADD, DIS, UPD, DELL					

Example: $DD-USER2

Privileges	PERSON	FACILITY	ENTITY-TYPE	STATUS	FUNCTIONS
Assigned	SECLVL=0	SECLVL=1	SECLVL=2	SECLVL=3	SECLVL=4
F=ALL	F=ALL	F=ALL	F=ALL	F=ALL	F=ALL
E=DATABASE (T005)	E=ALL	E=ALL	E=DATABASE TEST	E=DATABASE	E=DATABASE
P=DIS, ALIAS	P=DIS ALL MNT TEST	P=DIS ALL MNT TEST	P=DIS ALL MNT TEST	P=DIS T005 MNT T005	P=DIS T005 ALIAS T005

Planning for CA Datacom Datadictionary Security

Planning the implementation of CA Datacom Datadictionary Security is an important step in the process of securing your CA Datacom Datadictionary resources. The components of planning are:

- Security strategy (The CA Datacom Datadictionary validation process you have selected for your site. See Security Level (SRT) (see page 90).
- Resources and users to secure
- Implications of CA Datacom Datadictionary Security on other areas of the product

Determining Security Strategy

Decide on the security level to implement at your site.

- 0 Person Level (minimum)
- 1 Facility Level (assigned level at installation)
- 2 Entity Level
- 3 Status Level
- 4 Function Level

Identifying Resources and Personnel to Secure

After you have identified the level of security to implement at your site:

1. Identify the users to authorize CA Datacom Datadictionary resource access. If you are using security level 0, this is all you need to do.
2. Classify these users into groups which need the same access to resources. For example:
   - A programming development staff needs retrieval access to TEST and PROD status.
   - A systems design staff needs update and retrieval access against TEST status, and retrieval access to PROD status.
   - The Database Administrator needs update access to PROD status.
3. If necessary, identify the profiles required for these groups and determine the following:
   - What facilities they need to use.
   - What entity-types they need to access.

- What entity-types they can access in a specific status.
- What functions they can perform on the associated entity-types in a specific status.

4. Assign the PERSON entity-occurrences to the appropriate profiles.

Implications of CA Datacom Datadictionary Security

Installing CA Datacom Datadictionary Security has implications on the following areas:

- Running CA Datacom Datadictionary Service Facility (DSF)
- Generic retrieval and retrieval of an entity-occurrence along a path
- Executing SQL statements in the Interactive SQL Service Facility

Running DSF

The entity-occurrences which you can retrieve for display or update purposes with DSF depend on the security level at your site and if you are authorized in your user profile. The user and optional password specified in the USRINITI command to DSF are validated against the PERSON entity-occurrence. If no match is found, access is denied. If a match is found, CA Datacom Datadictionary Security uses the profile for that user to determine the access rights of your DSF program. The Security Administrator defines the DSF USRINITI user name as a PERSON entity-occurrence. For more information about these procedures, see Maintaining Persons (see page 159) and Updating Profiles (see page 150).

Retrieving Entity-Occurrences

When you retrieve entity-occurrences of multiple entity-types, you receive *only* the entity-occurrences of the entity-types you are authorized to access. All the other defined entity-occurrences are ignored.

For example, suppose your CA Datacom Datadictionary contains PROGRAM entity-occurrences A and B, and SYSTEM entity-occurrences X and Y. However, you have authorization to access only the PROGRAM entity-type. A CA Datacom Datadictionary online request to display an index of all entity-types would result in a display that includes PROGRAM entity-occurrences A and B. It would not show SYSTEM entity-occurrences X and Y.

In another example, suppose you request a path report through CA Datacom Datadictionary batch processing for an Index Report of the ORDER-ENTRY database and you only have access to DATABASE and TABLE entity-types. When you submit the following batch reporting commands, you would receive the following reports:

```
-USR SAMPLE-USER,PSWD
-DEF PATH,STANDARD
-END
-RPT START,DATABASE,ORDER-ENTRY(PROD),STANDARD
-RPT INDEX
-END
```

For an example report header, see Sample Report Headers.

The following are examples for pages 1 through 5.

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

             *-------------------------------------------------------------------------------*
             *  CODE USER-NAME,PSWD,DATABASE-ID                                              *
             *  -USR SAMPLE-USER,****                                              ;00PROC   *
             *-------------------------------------------------------------------------------*
```

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

-DEF PATH,STANDARD
-END
```

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

-RPT START,DATABASE,ORDER-ENTRY(PROD),STANDARD
-RPT INDEX
-END
```

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

ENTITY-TYPE..................... OCCURRENCE..................... VRSN STS LK PSWD DESCRIPTION.........................
   RECORD.........................     ELEMENT.......................

DATABASE                         ORDER-ENTRY                     0003  P   0      ORDER-ENTRY DEMO DATABASE
TABLE                            ACCTS                           0003  P   0      ORDER-ENTRY ACCTS TABLE
TABLE                            CUST                            0003  P   0      ORDER-ENTRY CUST TABLE
TABLE                            DETAIL                          0003  P   0      ORDER-ENTRY DETAIL TABLE
TABLE                            ORDERS                          0003  P   0      ORDER-ENTRY ORDERS TABLE
TABLE                            ITEMS                           0003  P   0      ORDER-ENTRY ITEMS TABLE
TABLE                            ORD-NO                          0003  P   0      ORDER-ENTRY ORDER-NUMBERS TABLE
TABLE                            RCPTS                           0003  P   0      ORDER-ENTRY RECEIPTS TABLE
TABLE                            SHIPTO                          0003  P   0      ORDER-ENTRY SHIP-TO TABLE
TABLE                            SLSHST                          0003  P   0      ORDER-ENTRY SALES-HIST TABLE
                                        *--------  E N D   O F   J O B  -----------*
```

The full structure Index Report would include the AREA, KEY, ELEMENT, and FIELD entity-occurrences.

When you request entity-occurrences of a specific entity-type you are not authorized to access, you receive a UNA (user not authorized) CA Datacom Datadictionary Service Facility (DSF) return code or a CA Datacom Datadictionary error message.

Interactive SQL Service Facility

Securing the Interactive SQL Service Facility does not secure your data. It secures the use of this mode in CA Datacom Datadictionary online.

Note: For more information on the Interactive SQL Service Facility, see the *CA Datacom/DB SQL User Guide*.

Once access to the facility is allowed, a user can have access to the data. You can secure access to data by using the GRANT and REVOKE functions in SQL processing. For more information, see CA Datacom SQL Security (see page 285).

Implementing CA Datacom Datadictionary Security

This section provides instructions on getting started and a step-by-step description of the tasks needed to implement CA Datacom Datadictionary Security.

Initial Security Administrator

When CA Datacom Datadictionary is installed there is a PERSON entity-occurrence supplied with the system:

- DATACOM-INSTALL - Name
- NEWUSER - Password

Note: DATCOMIN is an alias that can be used as a short form of DATACOM-INSTALL USER in r12. It can be used in place of the longer name if your site has a user ID length restriction of eight (8) characters or less. DATACOM-INSTALL is the user name for the CA Datacom Datadictionary ++USR statement as listed in the z/OS Installation Worksheet.

This entity-occurrence is established as a Security Administrator and with full access to all entity-types installed. You can use the identification to access the Security Maintenance facility to establish your own Security Administrators. Once this is done, either delete the PERSON entity-occurrence DATACOM-INSTALL, modify the NEWUSER password, or removed the Security Administrator authority.

Installing CA Datacom Datadictionary Security

You should have completed the planning of CA Datacom Datadictionary Security as described in Planning for CA Datacom Datadictionary Security (see page 106) before beginning implementation.

Step 1

If you select a security level greater than 1 - Facility Level, or if you select no CA Datacom Datadictionary Security (0), you must change the SECLVL= parameter in the System Resource Table (SRT) after installing this version.

Five options are available:

Option 0:

Enforces minimum security in CA Datacom Datadictionary. Only the presence of a PERSON entity-occurrence in PROD status is required for access to most facilities of CA Datacom Datadictionary.

Option 1: FACILITY LEVEL (default)

A user must be authorized to use a *given* facility (DDUPDATE, DDUTILTY, ENTM, SQL, and so on).

Option 2: ENTITY LEVEL

A user must be authorized to perform any function on a *given* entity-type.

Option 3: STATUS LEVEL

A user must be authorized to perform any function on a *given* entity-type in a *given* status.

Option 4: FUNCTION LEVEL

A user must be authorized to perform a *given* function, on a *given* entity-type, in a *given* status.

Step 2

Accept the default for the COMPAT= parameter in the CA Datacom Datadictionary System Resource Table.

Note: For more information about this parameter, see the *CA Datacom/DB Database and System Administration Guide*.

Step 3

Using the CA Datacom Datadictionary Security Maintenance facilities, enter the profiles and catalog them to the High-Speed Directory (HSD).

Step 4

Also using the CA Datacom Datadictionary Security Maintenance facilities, identify the users to the system and associate each with a profile. In addition, a user can optionally be assigned as a CA Datacom Datadictionary Security Administrator.

Using CA Datacom Datadictionary Online Security Maintenance

Before using CA Datacom Datadictionary Security, you must have a basic understanding of CA Datacom Datadictionary online. The following describes how to maneuver through online CA Datacom Datadictionary from the Authorization Mode viewpoint.

Note: For more information, see the *CA Datacom Datadictionary Online Reference Guide*.

The major topics covered in this chapter are:

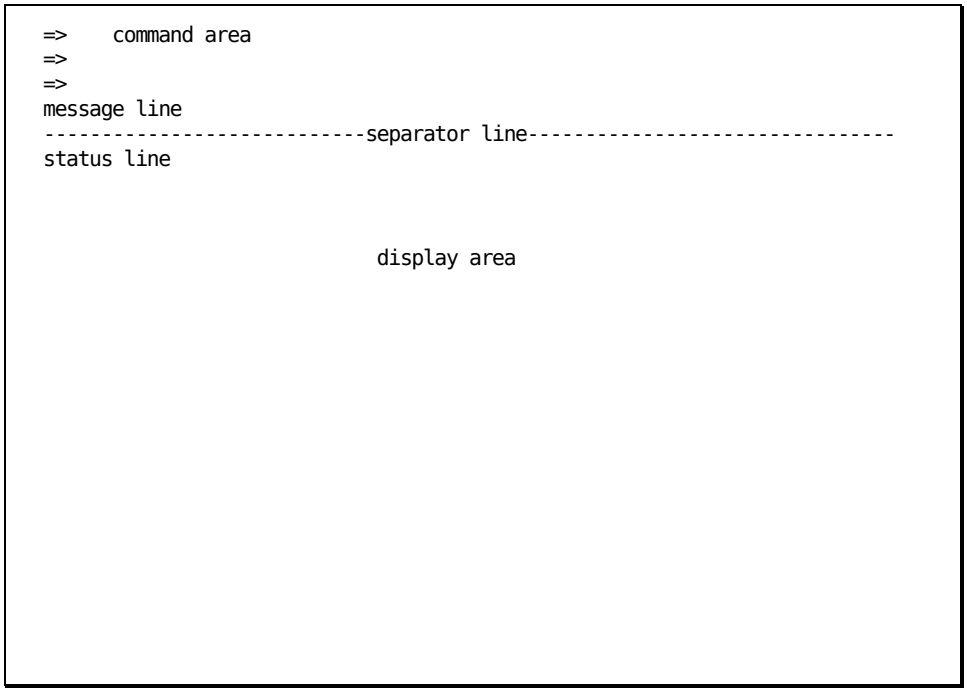
- Signing on and off
- Types of panels
- Split screen capability
- HELP processing
- Updating CA Datacom Datadictionary
- Naming standards
- Processing sequence
- Command processing
- Line commands
- Online work queue

Types of Panels

CA Datacom Datadictionary uses the CA IPC to simplify management of panels, screen data, and commands. Various other CA products also use the CA IPC. This allows multiple CA products to run concurrently at the same terminal and provide a set of services that are common to those products. These services include:

- Usage authorization (SIGNON/SIGNOFF)
- Driving of menus and other panels
- Program function key (PF) analysis
- Support for multiple commands in the same line of commands
- Multiple lines of commands
- HELP functions
- Processing of error or informative messages
- Support of asynchronous tasks
- Debugging facilities

Following is the arrangement of a typical CA Datacom Datadictionary screen layout.



The organization of the CA Datacom Datadictionary screen is:

command area

The top lines of the screen, each with a line indicator symbol (=>), where you can enter commands.

CA Datacom Datadictionary is installed with a default of three lines. You can modify the number of lines available in the command area with the SET CMD LIN *n* command, where *n* is the number of lines in the command area from 5 to 0. If you set the number of command lines to 0, you must use the function keys and menu selections to move from panel to panel and to perform CA Datacom Datadictionary functions. For more information about entering commands, see Using Command Processing (see page 119).

message line

The area where messages are displayed. If you set the command area to 0, the message line is at the top of the panel.

separator line

The line of dashes below the command area that separates the command area from the display area. You can change the dashes to another character with the SET CMD SEP *c* command, where *c* is the character.

status line

The line that describes the contents of the display area. This line consists of either the name of the selected mode or the function selected on a main menu of a processing mode.

display area

A portion of the screen that contains varying information depending on the type of panel. The types of panels used in CA Datacom Datadictionary are:

- Menu panels
- Prompter panels
- Display panels
- Maintenance panels

Processing is accomplished by entering the requested data on the panel and then using a command, the Enter key, or both as required by the panel, to transmit the entries to CA Datacom Datadictionary. Some commands can be transmitted by pressing program function (PF) keys.

When processing is completed for one panel, CA Datacom Datadictionary either displays a message on the current panel or displays the next logical panel, according to the outcome of processing. If an error is encountered during processing, CA Datacom Datadictionary displays an error message.

Menu Panels

A menu panel allows you to select from a list of options rather than enter a command. In many cases, you can skip the menu panels by entering the appropriate command. Valid options or functions are listed on the menu and a brief description is given. Most menus include the abbreviated command syntax.

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          P04M
Enter desired option number ===> __    (There are 11 options on the menu)

 1. MAINTAIN PERSON       (MNT PER)     Maintain PERSON definitions
 2. ADD PROFILE           (A PROF)      Add a PROFILE
 3. UPDATE PROFILE        (U PROF)      Update a PROFILE
 4. DELETE PROFILE        (DEL PROF)    Delete a PROFILE
 5. CATALOG PROFILE       (CAT PROF)    Catalog a PROFILE
 6. DISPLAY PERSON        (D PER)       Display PERSON definitions
 7. DISPLAY INDEX PROFILE (D I PROF)    Display a PROFILE Index
 8. DISPLAY USAGE PROFILE (D USE PROF)  Display a PROFILE Usage
 9. DISPLAY DEF PROFILE   (D DEF PROF)  Display a PROFILE definition
10. SET MODE                            Reset DATADICTIONARY processing mode
11. OFF                                 End session
```

You can select an option on the menu panel by either typing the option number in the designated field in the display region and pressing Enter, or by typing the command for the option in the command region and pressing Enter. CA Datacom Datadictionary then displays another menu or a prompter panel where you can enter specific criteria for the function you want to perform.

Prompter Panels

A prompter panel contains the proper command syntax for the selected function. It displays both the long and abbreviated command syntax. Prompter panels assist new users unfamiliar with the CA Datacom Datadictionary commands or a user unsure of the proper syntax.

On a prompter panel, you supply the variable information about the entity-occurrence. The required entries are highlighted.

```
 =>
 =>
 =>
 --------------------------------------------------------------------------------
 DATADICTIONARY Security Maintenance

T40F
 UPDATE   PROFILE    _____________________________
 UPD      PROF      (name)


             ENTITY  _____________________________
             ENT        (type)
```

After filling in all required fields and any desired optional fields on a prompter panel, submit the command to CA Datacom Datadictionary by either pressing the Enter key or entering the APPLY command, depending on the function performed by the prompter panel.

You can enter the APPLY command by typing APPLY, or APP, on a command line and pressing Enter, or by pressing PF9. For more information, see Using Command Processing (see page 119) and Using PF and PA Keys (see page 118). CA Datacom Datadictionary responds with the next logical panel for the function, a message confirming successful completion of the function, or an error message.

Display Panels

A display panel provides user-requested information or CA Datacom Datadictionary initiated information, such as the result of an APPLY command. You can use a display panel to obtain information about users or profiles. You can enter specific commands in the line numbers at the left margin on a display panel. For more information, see Using the Online Work Queue (see page 138).

The following section shows the Profile Index panel. There are other displays available, such as displays of a security profile definition or usage, or of a PERSON entity-occurrence's security profile. Security profile definitions and usage are described in Displaying Profile Definitions (see page 155) and Displaying Profile Usage (see page 157).

Profile Index Display

You can use the Profile Index display to display all CA Datacom Datadictionary profiles available at your site. The following is an example of the Profile Index Display panel:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T47D
       Profile Index
====== ======================== T O P ===================================
000001 $DD-ADM
000002 $DD-COP
000003 $DD-DIS
000004 $DD-PROGRAMMER
000005 $DD-SEC-ADM
000006 $DD-UPD
====== ===================== B O T T O M ================================




PF1=HELP   PF2=END   PF3=CLARIFY   PF4=PROCESS   PF5=MENU    PF6=STATUS
PF7=SCB    PF8=SCF   PF9=APPLY     PF10=PATH     PF11=NEXT   PF12=INPUT
```

When a display extends beyond the bottom of your screen, you can use the scrolling commands or PF7 and PF8 to move through the display. For more information, see Using PF and PA Keys (see page 118).

Maintenance Panels

Use a maintenance panel to add or change attribute values, define profiles, and assign profiles to users. All Security Maintenance panels are variable line panels. A variable line panel contains repeating groups. A repeating group is a collection of contiguous fields treated as a unit. These contiguous fields can span more than one line on the panel.

Repeating groups can be inserted, copied, replicated, moved, and deleted. For more information and the line commands you can use with repeating groups on specific types of panels, see Using Line Commands (see page 137).

The following panel shows a line inserted after entering an I (insert) line command and the new data that the user has entered:

```
 => apply
 =>
 =>

 ------------------------------------------------------------------------------
 DATADICTIONARY Security Maintenance
                                                                          T41U
 ............................... PERSON ATTRIBUTES ........................

OPTIONAL:Enter Specific Person- ____________________________________
        Name                                                    Sec.
         User-Password     ID  Profile                        Admin.
 000001 DATACOM-INSTALL
                           $DD-ADM                            Y
 ...... JOHN-SMITH_____________________

                           JS1 $DD-ADM_____________________________ Y

 ====== ====================== B O T T O M   ================================



 PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS
 PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

Updating CA Datacom Datadictionary

You update CA Datacom Datadictionary by entering data on a panel or with a command. This data is stored in a work file until processed with the APPLY command (PF9). The CA Datacom Datadictionary Online Work File (DDOFILE) is used to store session-dependent information over a logical process that can span the processing of several panels of information. The work file is a Virtual Library System (VLS) file.

When you issue the APPLY command, either in the command region or with PF9, the CA Datacom Datadictionary database is updated with the information in the work file.

Note: The CA Datacom Datadictionary database is *never* updated until the APPLY command is processed.

Using PF and PA Keys

CA Datacom Datadictionary is installed with preset PF and PA keys. For terminals with more than 12 program function keys, PF13 through PF24 correspond to PF1 through PF12.

The PF and PA keys perform the following functions except in the Interactive Service Facility Mode, in the Interactive SQL Service Facility Mode, or on a HELP panel. For those assignments, see the *CA Datacom Datadictionary User Guide* or *CA Datacom Datadictionary Online Reference Guide*. Equivalent commands and abbreviated commands (if applicable) are listed with the PF key definition.

Key	Equivalent Command and Action
PF1	HELP (HEL) - displays current HELP panel.
PF2	END - terminates processing, clears anchored entity-occurrences and returns to the main menu for the current mode.
PF3	CLARIFY - provides more information when the message "One or more fields in error. Use 'Clarify' for details." is displayed.
PF4	PROCESS (PRO) - retrieves and executes the next entity-occurrence and function from the online work queue.
PF5	MENU (MEN) - terminates processing, remains anchored on selected entity-occurrence and returns the main menu for the current mode.
PF6	STATUS (STA) - displays the Datadictionary Session Status Display panel that shows session status and anchored entity-occurrence information.
PF7	SRB - scrolls backward the number of lines in the repeating group section of the displayed variable panel.
PF8	SRF - scrolls forward the number of lines in the repeating group section of the displayed variable panel.
PF9	APPLY (APP) - applies updates entered through the processing panel and activates the next logical panel.
PF10	PATH (PAT) - selects the next entity-occurrence along the defined path.
PF11	NEXT (NEX) - selects the next entity-occurrence that meets the selection criteria AUTHORIZE, DBMAINT, and ENTDISPL modes, and for TEXT processing in ENTMAINT Mode.

PF12 INPUT (INP) - valid only on Text Maintenance panels – opens a window of blank lines on the Text Maintenance panel for the addition of more text. For more information, see the SET WINDOW command in the *CA Datacom Datadictionary User Guide*.

NEXT CLASS (NEX CLS) - valid only on Text Display panels - if you enter ALL for the Text Classification parameter on the Selection Criteria Fill-in panel, displays the next Text Classification in alphabetical order when there is more than one.

PA1 Refreshes screen.

PA2 Displays PF/PA key assignments.

Clear Same as PF2.

Enter Performs different functions on various panels:

- On display panels: processes margin and line commands and refreshes the screen. This allows you to specify additional margin commands.
- On variable line maintenance panels: executes any line commands you type in the line numbers and refreshes the screen.
- On prompter panels and menu panels: displays the next panel when there is a series of panels.
- On Selection Criteria panels: performs the function you have selected or displays the next panel in a series of panels.

Using Command Processing

You can use the CA Datacom Datadictionary commands to perform the following functions:

- Call various panels bypassing the set of menus and prompter panels
- Scroll through a display
- Manipulate data
- Process updates

The abbreviated command syntax for the menu options is displayed on the panels so you can learn the commands easily. The full and abbreviated command syntax for functions performed by the prompter panels are displayed on those panels. You can skip the prompter panel by entering these commands. However, if the complete command is longer than the 76 spaces available in a command line, use the prompter panel. A command cannot be continued to another line.

To issue commands to CA Datacom Datadictionary, enter the command in the command region at the top of the panel and press Enter. The commands documented here are valid in the AUTHORIZE processing mode.

Note: For more information and a description of CA Datacom Datadictionary command processing in other modes, see the *CA Datacom Datadictionary Online Reference Guide*.

Except where noted, you can enter more than one command on a panel as shown in the following examples. You can change the number of command lines displayed with the SET CMD LIN command.

Note: For more information about setting session defaults, see ADD PROFILE (see page 121) and the *CA Datacom Datadictionary Online Reference Guide*.

- You can type each command on a separate line.

```
==> apply
==> end
==>
```

- Or, you can type several commands on the same line and separate them with a semicolon (;), the default delimiter. (For more information about changing the delimiter with the SET CMD DLM command, see the *CA Datacom Datadictionary User Guide*.)

```
==> apply;end
==>
==>
```

When you enter only a part of a command, CA Datacom Datadictionary presents the prompter panel or menu for that function with the information you have filled in on the panel. For example, if you enter the incomplete command, ADD PROFILE, in the command area of the DATACOM/DD Security Maintenance Menu, CA Datacom Datadictionary presents the following prompter panel for you to complete the required information.

```
 =>
 =>
 =>

--------------------------------------------------------------------------------
 DATADICTIONARY Security Maintenance
                                                                          T40F
 ADD      PROFILE    _________________________________
 ADD      PROF       (name)
```

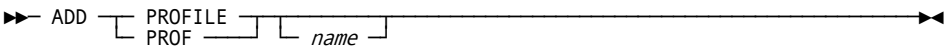
Remember that on a prompter panel, you must do the following:

- Supply all required entries.
- Supply any desired optional entries.
- Press Enter or PF9 (APPLY) to continue processing.

ADD PROFILE

Use the ADD PROFILE command to add a profile to CA Datacom Datadictionary. When you do not include the occurrence-name with the command, CA Datacom Datadictionary displays the Add Profile Prompter panel. For more information, see Adding CA Datacom Datadictionary Profiles (see page 142).

Use the following format for this command:



name

(Optional) The AUTHORIZATION entity-occurrence name of the profile you are adding. The name, if entered, must begin with $DD-.

Valid Entries:

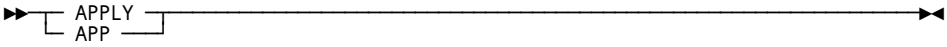
1 to 32 characters

Default Value:

(No default)

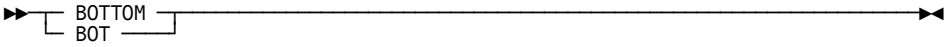
APPLY

Use the APPLY command to update CA Datacom Datadictionary with the data entered on a maintenance panel. APPLY is also a valid command from several prompter panels. Use the following format for this command:



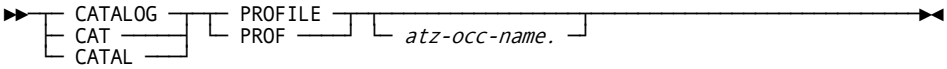
BOTTOM

Enter the BOTTOM command to scroll to the last panel display of a variable panel. You can use this function in all modes. Use the following format for this command:



CATALOG PROFILE

Use the CATALOG PROFILE command to post the definition of a profile to the CA Datacom Datadictionary High-Speed Directory (HSD). If you do not enter a name, CA Datacom Datadictionary displays the Catalog Profile Prompter panel for you to enter the information. For more information about this panel, see Cataloging Profiles (see page 147). Use the following format for this command:



atz-occ-name.

(Optional) The AUTHORIZATION entity-occurrence name of the profile you are cataloging. The name, if entered, must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

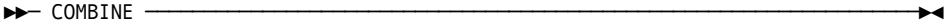
Press PF9 or type **APPLY** to catalog the profile to the HSD.

If the CATALOG function is successful and no errors are detected, CA Datacom Datadictionary displays the DATACOM/DD Security Maintenance Menu with a message indicating successful completion of this function.

If the CATALOG function fails due to errors, CA Datacom Datadictionary displays an error panel that contains messages that can be used to diagnose the errors in the structure.

COMBINE Command

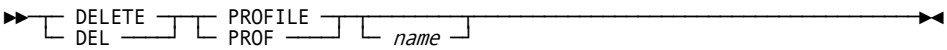
Use the COMBINE command to terminate the bottom region of a split screen and give its area to the region displayed above it. Do not stack this command with commands that process data, such as the APPLY command.



DELETE PROFILE

Use the DELETE PROFILE command to delete a profile from CA Datacom Datadictionary. When you do not include the occurrence-name with the command, CA Datacom Datadictionary displays the Delete Profile panel. For information about this panel, see Deleting Profiles (see page 149).

Use the following format for this command:



name

(Optional) The AUTHORIZATION entity-occurrence name of the profile you are deleting. The name, if entered, must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

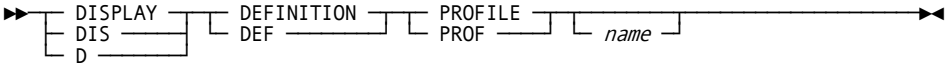
(No default)

DISPLAY DEFINITION PROFILE

Use the DISPLAY DEFINITION PROFILE command to display profile definitions. This function is useful when you need to know how a particular Profile is set up before relating a new PERSON entity-occurrence, or prior to updating the profile definition.

If you omit the optional profile name, CA Datacom Datadictionary displays the Display Definition Prompter panel for you to enter this information. For more information about this panel, see Displaying Profile Definitions (see page 155).

Use the following format for this command.



name

(Optional) The AUTHORIZATION entity-occurrence name of the profile you want to display. The name, if entered, must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

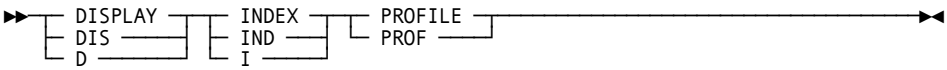
(No default)

When you press Enter, CA Datacom Datadictionary responds with the profile definition requested.

DISPLAY INDEX PROFILE

Use the DISPLAY INDEX PROFILE command to display an index of CA Datacom Datadictionary Security profiles.

Use the following format for this command:



When you press Enter, CA Datacom Datadictionary responds with an index of the profiles defined to the system. You can enter margin commands in the line numbers of the profiles on the panel.

The following are the valid margin commands you can enter on this panel. For more information about using margin commands, see Using the Online Work Queue (see page 138).

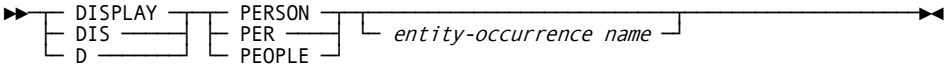
Margin Command	Description
CAT	Catalog a Profile
DDF	Display a Profile Definition
DEL	Delete a Profile
DUS	Display Profile Usage
UPD	Update a Profile

DISPLAY PERSON

Use the DISPLAY PERSON command to display authorization information for one PERSON entity-occurrence and information on the profile to which the PERSON entity-occurrence is related. This function is useful when you need to know the profile authorizations for a particular person.

If you omit the optional PERSON entity-occurrence name, CA Datacom Datadictionary displays the Display Person Prompter panel for you to enter this information. For more information about this panel, see Displaying Person Definitions (see page 152).

Use the following format for this command:



entity-occurrence name

(Optional) Limit the definition to a single entity-occurrence by entering the name of the entity-occurrence. You can enter ALL for all occurrences or a generic selection using 1 through 31 characters of an occurrence name and an asterisk (*). For example, ACC* processes all occurrences of this entity-type with ACC as the first three characters in the name.

Valid Entries:

1 to 32 characters
Generic selection
ALL

Default Value:

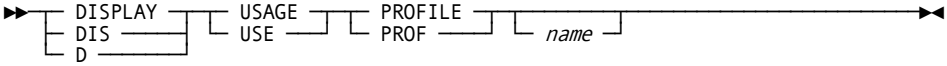
ALL

When you press Enter, CA Datacom Datadictionary responds with the PERSON entity-occurrence definition requested.

DISPLAY USAGE PROFILE

Use the DISPLAY USAGE PROFILE command to display a list of PERSON entity-occurrences assigned a specific profile.

If you omit the optional profile name, CA Datacom Datadictionary displays the Display Usage Prompter panel for you to enter this information. For more information about this panel, see Displaying Profile Usage (see page 157). Use the following format for this command:



name

(Optional) The AUTHORIZATION entity-occurrence name of the profile you want to display. The entity-occurrence name, if entered, must begin with $DD-.

Valid Entries:

1 to 32 characters

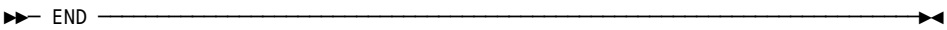
Default Value:

(No default)

When you press Enter, CA Datacom Datadictionary responds with the requested information.

END

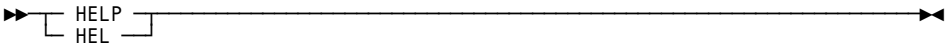
Use the END command to terminate processing and return to the menu for the current mode. You can use this command in all processing modes.



When you press Enter, CA Datacom Datadictionary displays the menu for the current processing mode.

HELP

Use the HELP command to display the current HELP panel. The HELP command is valid in all modes. You can enter the HELP command on any panel. Use the following format for this command:

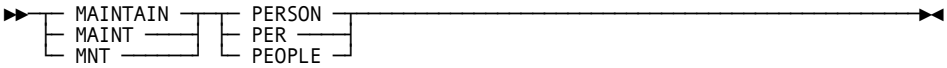


MAINTAIN PERSON

Use the MAINTAIN PERSON command to display a list of PERSON entity-occurrences defined to the system. CA Datacom Datadictionary responds with the Maintain Person panel.

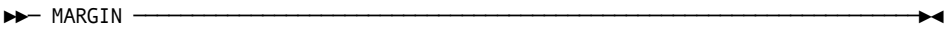
You can add, delete, or change the PERSON entity-occurrence definitions by using line commands or by typing over the information you want to change.

Use the following format for this command:



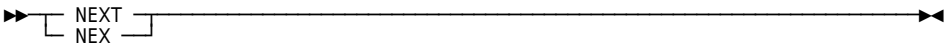
MARGIN

Use the MARGIN command to display a list of the margin commands you can use to establish an online work queue. For more information, see Using the Online Work Queue (see page 138).



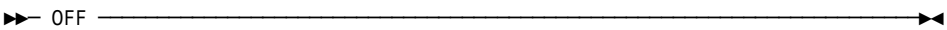
NEXT

Use the NEXT command in AUTHORIZE, DBMAINT, and ENTDISPL Modes and for TEXT processing in ENTMAINT Mode to obtain the next entity-occurrence that meets the criteria you specified. Use the following format for this command. You can also issue the NEXT command with the PF11 key.



OFF

Use the OFF command to terminate processing and sign off CA Datacom Datadictionary. This command is valid in all processing modes.



When you press Enter, CA Datacom Datadictionary presents the CA Datacom Datadictionary signoff panel.

- If you have entered data on a panel and have not issued the APPLY command, the CA Datacom Datadictionary database is not updated and the data is lost. For more information, see Updating CA Datacom Datadictionary (see page 117).
- If you have entered margin commands but have not processed them, they are lost when you sign off. For more information, see Using the Online Work Queue (see page 138).

OFFON

Enter the OFFON command to sign off CA Datacom Datadictionary and sign on again. This can be helpful when you want to sign on with a different user ID, or when you want to sign on to a different CA Datacom Datadictionary. You can establish specific user IDs for specific levels of authorization to perform specific functions. You can have multiple CA Datacom Datadictionarys at one site.

When you press Enter, CA Datacom Datadictionary presents the CA Datacom Datadictionary signon panel.

If you have entered data on a panel and have not issued the APPLY command, the CA Datacom Datadictionary is not updated and the data is lost. For more information, see Updating CA Datacom Datadictionary (see page 117).

If you have an uncompleted work queue, it is lost when you sign off. For more information, see Using the Online Work Queue (see page 138).

PROFILE

Use the PROFILE command to display the Security Profile panel. This panel displays the authorizations assigned to the user identification code with which you signed on to the current session of CA Datacom Datadictionary. For more information about assigning authorizations, see the sections about adding, deleting, updating, and cataloging profiles in this guide.

Use the following format for this command:

When you press Enter, CA Datacom Datadictionary presents a panel similar to the following example. You cannot update the attribute-values on this panel.

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Profile                                          PRFH
DISPLAY PERSON: USERNAME                          User-Password: PSWD
 User-ID: UID  Profile: $DD-ADM                          Security Admin.: Y

.......................... FACILITY LEVEL SECURITY ..........................
Online Facilities - ( DBM: Y   FMM: Y   ENTM: Y   ENTD: Y   ISF: Y   SQL: Y )
Batch  Facilities - ( UPD: Y   UTL: Y    CFB: Y    BTG: Y   RMF: Y   TRS: Y )

........................... ENTITY LEVEL SECURITY ............................
                                 D A D U  F   R S  V D E C  D T A D  R S S O
      Entity              All    i d e p  r T e e  e s n a  e x l e  e e t b
             Status   Functions? s d l d  m o s t  r a a t  f t s s  l c a s
====== ======================== T O P ====================================

000001 AREA
               PROD        Y      Y Y Y Y  Y Y Y Y  Y Y Y Y  Y Y Y Y  Y Y Y Y
000002 AUTHORIZATION
               PROD        Y      Y Y Y Y  Y Y Y Y  Y Y Y Y  Y Y Y Y  Y Y Y Y
```

DISPLAY PERSON:

Specifies the full name associated with the user ID used on the CA Datacom Datadictionary signon panel for this session.

User-Password:

Specifies the password, if any, assigned to this user ID.

User-ID:

Specifies the user identification you accepted or entered on the CA Datacom Datadictionary signon panel for this session. You can have many different user identifications, for example, for different functions.

Profile:

Specifies the entity-occurrence name of the related $DD- AUTHORIZATION entity-occurrence.

Security Admin.:

Indicates with the letter Y (yes) if this user ID is authorized as a CA Datacom Datadictionary Security Administrator (profile $DD-SEC-ADM).

Facility Level Security section

Indicates with the letter Y (yes) that authorization is associated with this user ID to use the following facilities:

ID	**Batch Facility**
BTG	DDBTGLM maintenance
CFB	DDCFBLD maintenance
RMF	DDRMFLM maintenance
TRS	DDTRSLM maintenance
UPD	DDUPDATE maintenance
UTL	DDUTILTY maintenance
ID	**Online Facility**
DBM	CA Datacom/DB Structure Maintenance
ENTD	CA Datacom Datadictionary Entity Display
ENTM	CA Datacom Datadictionary Entity Maintenance
FMM	File Structure Maintenance
ISF	Interactive Service Facility
SQL	Interactive SQL Service Facility

Entity Level Security section

Contains a list of the function authorizations associated with this user ID for specific entity-types in a specific status.

Entity

The entity-type name.

Status

The status of the entity-type.

All Functions?

Indicates with the letter Y (yes) or N (no) if all functions are authorized for this entity-type in this status.

Specific Functions

Under the following abbreviations, the letter Y (yes) or N (no) indicates if the function is authorized for this entity-type in this status.

Note: The abbreviations for the functions that can be performed against an entity-type are displayed vertically on the panel.

Heading	Function	Heading	Function
Add	ADD/CREATE	Obs	OBSOLETE
Als	ALIAS maintenance	Rel	RELDEF/TRANSFER
Cat	CATALOG	Res	RESTORE
Def	DEFINE	Sec	PASSWORD/LOCK maintenance
Del	DELETE/REMOVE	Set	SET
Des	DESCRIPTOR maintenance	Sta	STATUS maintenance
Dis	DISPLAY	To	COPY TO
Dsa	DISABLE	Txt	TEXT maintenance
Ena	ENABLE	Upd	UPDATE/MODIFY
Frm	COPY FROM	Ver	VERIFY

SCROLL

Use the SCROLL command to move forward and backward through the lines of a panel that you cannot display all at one time on a single screen. Use the following format for this command.

If you do not add a keyword with the SCROLL command, CA Datacom Datadictionary scrolls the display forward the set number of lines in a region with the last line of the previous display at the top of the new display. You can also enter this command with the PF8 key.

You can add the following optional keywords to the SCROLL command.

Command	Action
+	Scroll forward the set number of lines in a region. (You can also use the PF8 key, the SCROLL command, or the SRF command for this function.)
	Scroll backward the set number of lines in a region. (You can also use the PF7 key or the SRB command for this function.)
+*nnn*	Scroll forward *nnn* number of lines in a region.
-*nnn*	Scroll backward *nnn* number of lines in a region.
B	Scroll backward the set number of lines in a region. (You can also use the PF7 key, the BACKWARD command, the SCROLL - command, or the SRB command for this function.)
F	Scroll forward the set number of lines in a region. (You can also use the PF8 key, the SCROLL command, the SCROLL + command, or the SRF command for this function.)
BOT	Scroll to bottom of the list. (You can also use the BOTTOM command for this function.)
TOP	Scroll to top of the list. (You can also use the TOP command for this function.)

SET

You can use the SET command in different ways depending on the online mode and the keywords used with the command. You can use this function with the appropriate keywords to assign certain default values, environment conditions, or the mode during the current session.

You use the SET DATABASE command to request CA Datacom Datadictionary to assign certain modifiable and nonmodifiable (those set internally by CA Datacom Datadictionary) attribute-values.

Note: For more information about the SET DATABASE command, see the *CA Datacom Datadictionary User Guide*.

Use the following commands to perform the described action:

SET AUTHID

Displays the AUTHORIZATION-ID Panel in the SQLADMIN function of the Interactive SQL Service Facility. Use the panel to change to a different AUTHID to be used as the default for the session.

Note: For more information about the Interactive SQL Service Facility and AUTHID, see the *CA Datacom/DB SQL User Guide*.

SET AUTHOR '*name*'

Specify the default setting for the AUTHOR attribute when defining entity-occurrences. The name must be enclosed in single quotes.

SET CMD DLM *c*

Change the command delimiter character, where *c* is the character. The default delimiter is a semicolon (;).

SET CMD LIN *n*

Change the number of lines for commands on panels, where n is the number of lines. Valid entries are 0-5. The default is three lines.

SET CMD RPT *c*

Change the command repeat character, where *c*is the character. The default is a dash (-).

SET CMD RSW *c*

Change the command reshow character, where *c*is the character. The default is a plus sign (+).

SET CMD SEP *c*

Change the separator character displayed on the line between regions in a split screen, where *c*is the character. For more information about the default, see the CA IPC documentation.

SET CONTROLLER '*name*'

Specify the default setting for the CONTROLLER attribute when defining entity-occurrences. The name must be enclosed in single quotes.

SET DBID = *nnnnn*

Change to a different CA Datacom Datadictionary with a different CA Datacom/DB database ID than the one specified in the system resource table, where *nnnnn* is the ID number.

SET LANGUAGE *language*

Specify the default language to display on a Copybook Display Panel in ENTDISPL or ENTMAINT Modes. The system default is COBOL.

ASM|ASSEMBLER

Specifies the Assembler copybook

COB|COBOL

Specifies the COBOL copybook

DR

Specifies the CA Datacom/DB Reporting Facility copybook

PLI

Specifies the PL/I copybook

SET MODE *type*

Specify a processing mode, index display format, or text display format. The types and actions are as follows:

AUTH

Transfer to the Security Maintenance Mode.

DBM

Transfer to the CA Datacom/DB Maintenance Mode.

ENTD

Transfer to the Datadictionary Entity Maintenance Mode.

ENTM

Transfer to the Datadictionary Entity Display Mode.

FMM

Transfer to the File Maintenance Mode.

ISF

Transfer to the Interactive Service Facility Mode.

INDEX

Allow CA Datacom Datadictionary to determine the number of lines needed per entry on an index display panel. Two lines are used for FIELD, KEY, and ELEMENT entity-occurrences. One line is used for all other entity-occurrences.

INDEX1

Specify one line per entry on index display panels. This suppresses the display of parent-name for FIELD, KEY and ELEMENT entity-occurrences.

INDEX2

Specify two lines per entry on index display panels. Parent-name is displayed for FIELD, KEY, and ELEMENT entity-occurrences. A blank line follows all other entity-occurrences.

NONUM

Specify text panel lines at 79 characters with no numbered margins.

NUM

Specify the text panel lines at 72 characters with numbered margins.

SQL

Transfer to the SQL Mode.

blank

Return to the Datadictionary Mode Select Panel.

SET NAME *name*

Establish the default type of value to display for the Field-Name field on a Field Summary Display Panel in the ENTDISPL or ENTMAINT Modes. Enter one of the following for name in this command. The system default is the CA Datacom Datadictionary entity-occurrence name.

ASM|ASSEMBLER

Display the Assembler name.

CMP|COMPILER

Display the Compiler name.

DD|DATADICT

Display the CA Datacom Datadictionary entity-occurrence name.

DESC

Display the FIELD entity-occurrence descriptive information in the DESCRIPTION attribute.

SET SQL *syntax-id*

Override the syntax level set with the SQLMODE= parameter in the Multi-User Facility Master List or previously changed with this command. The change is valid for the duration of the current session. You cannot change this setting to DATACOM if SQLMODE=ANSI or SQLMODE=FIPS. For an explanation of conformance levels, see the *CA Datacom/DB SQL User Guide*. Enter one of the following:

ANSI

Conform to ANSI standard.

DATACOM

Conform to CA SQL extension.

FIPS

Conform to FIPS standard.

OFF

Return to default.

SET PREFIX = *name*

Specify 1 to 15 characters for CA Datacom Datadictionary to add to the beginning of each entity-occurrence name you define on panels in the ENTMAINT Mode. You can terminate your prefix setting with the RESET PREFIX command.

Note: For more information, see *CA Datacom Datadictionary Online Reference Guide*.

SET TEXT *class-name*

Specify the default value that CA Datacom Datadictionary will use for the classification name for the text you add to entity-occurrences.

Note: For more information about updating text, see the *CA Datacom Datadictionary Online Reference Guide*.

The system default is STANDARD.

The name can be up to 32 characters and must follow the CA Datacom Datadictionary naming conventions.

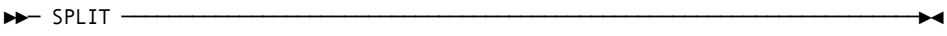
SET WINDOW = *nn*

Change the number of lines inserted with the INPUT command on a Text Maintenance Panel, where *nn* is the number of lines (window). The window must be at least 1 and can be a maximum of 2 less than the region size. The default is 5.

SPLIT

Depending on the type of terminal you have, you can use the SPLIT command to present more than one display area at the same time. This allows you to display different CA Datacom Datadictionary panels simultaneously or to access CA Datacom Datadictionary in one area and another product, such as CA Ideal, in the other area.

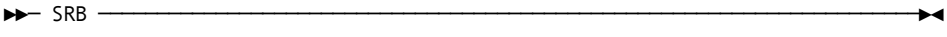
Note: For more information about this online command, see the *CA Datacom Datadictionary Online Reference Guide*. You cannot abbreviate this command.



Use the COMBINE command to terminate the bottom region of a split screen and give its area to the region displayed above it. Do not stack this command with commands that process data, such as the APPLY command.

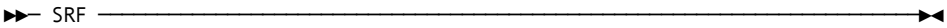
SRB

Use the SRB command to scroll the display area backward one panel in a region. The PF7 key also performs this function.



SRF

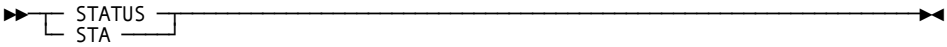
Use the SRF command to scroll the display area forward one panel in a region. The PF8 key also performs this function.



STATUS

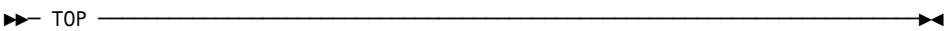
Use the STATUS command to display the Datadictionary Session Status Display panel. The panel shows CA Datacom Datadictionary session status and anchored entity-occurrence information.

Note: For the display and description, see the *CA Datacom Datadictionary Online Reference Guide*.



TOP

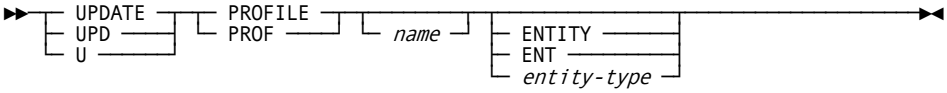
Use the TOP command to scroll a display area so that line 1 is the first line in the display area.



UPDATE PROFILE

Use the UPDATE PROFILE command to display information for a specific profile. You can display the appropriate Update Profile panel based on the keywords. Add, delete, or change profile information by using line commands or by typing over the information you want to change on these panels.

Use the following format for this command:



name

(Optional) The AUTHORIZATION entity-occurrence name of the profile you are updating. If you enter the entity-occurrence name, CA Datacom Datadictionary displays the Update Profile panel. This panel lists authorizations for facilities and all entity-type/status combinations defined to this profile. For more information about maintaining profile information using this panel, see Updating Profile Entity-Types (see page 169).

The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

entity-type

(Optional) The entity-type name. If you enter the entity-type name, CA Datacom Datadictionary displays the Update Profile Entity-Type panel that displays Entity Level Security for the specified entity-type. For more information about maintaining profile entity-type information using this panel, see Updating Profile Entity-Types (see page 169).

Valid Entries:

Valid CA Datacom Datadictionary long name for the entity-type.

Default Value:

(No default)

More information:

Maintaining Persons (see page 159)
Using Line Commands (see page 137)
Updating Profiles (see page 163)

Using Line Commands

Line commands can be used to scroll through, insert, copy, move, and delete lines in repeating groups on panels. These commands are not related to the online work queue commands which are called margin commands. For more information about these commands, see Using the Online Work Queue (see page 138). The numerical factor described with the following commands can be either left or right of the command depending on the site option selected.

For example, to insert three lines, enter either I3 or 3I depending on the value for the LCREP= parameter in the System Resource Table. This applies to the Delete, Insert, Move, Repeat, and Copy commands.

You can use the following line commands on Security Maintenance panels:

Command	Action
*	Scroll the display until this line is at the top of the panel.
+_nnn_	Scroll the display until the line that is *nnn* lines after this line is at the top of the panel.
-_nnn_	Scroll the display until the line that is *nnn* lines before this line is at the top of the panel.
A	Designate the location after which lines are to be copied or moved.
B	Designate the location before which lines are to be copied or move.

C	Copy a line. Use A or B to designate the location where the line is to be copied.
CC	Copy a block of lines. CC must be entered on the first line and the last line of the block. Use A or B to designate the location where the block is to be copied.
D	Delete a line.
DB	Delete all lines from this line through the bottom line.
DD	Delete a block of lines. DD must be entered on the first line and the last line of the block.
DT	Delete all lines from this line through the top line.
IB	Inserts a blank line before the first line.
I or I*n*	Insert lines. If used alone, only one unnumbered line is inserted into the panel after the line where the command is entered. If used with *n, n* number of unnumbered lines are inserted into panel after the line where the command is entered.
R or R*n*	Repeat lines. If used alone, only one line is repeated after the line where the command is entered. If used with *n*, the line where the command is entered is repeated *n* times after itself.
RR	Repeat a block of lines. RR must be entered on the first line and the last line of the block. The lines are repeated after the line of the designated block.

Using the Online Work Queue

The online work queue is a temporary set of entity-occurrences and functions for additional processing. You establish the work queue by entering margin commands on the Profile Index panel.

For example, on the following Profile Index panel, the CAT (CATALOG PROFILE) margin command places the profile in the online work queue to catalog the profile to the CA Datacom Datadictionary High-Speed Directory (HSD). The DDF (DISPLAY PROFILE DEFINITION) margin command places the profile in the work queue to display profile definitions.

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T47D
        Profile Index
====== ======================== T O P ========================================
000001 $DD-ADM
000002 $DD-COP
000003 $DD-DIS
CAT004 $DD-PROGRAMMER

000005 $DD-SEC-ADM
DDF006 $DD-UPD

====== ====================== B O T T O M ==================================



PF1=HELP   PF2=END   PF3=CLARIFY   PF4=PROCESS   PF5=MENU    PF6=STATUS
PF7=SCB    PF8=SCF   PF9=APPLY     PF10=PATH     PF11=NEXT   PF12=INPUT
```

Building a Work Queue

To place an entity-occurrence on the work queue, type a margin command in the line number for that entity-occurrence and press Enter. You can enter multiple margin commands on one or more panels. As your margin commands are processed, each entity-occurrence and function is added to the queue in logical sequence. The queue can contain entity-occurrences of any entity-type.

The work queue is available only for the duration of a session. The queue is not retained if you do not process all the entity-occurrences in the queue before the session is terminated. Rebuild the queue when you sign on if you want to process those entity-occurrences that were not processed in the previous session.

Margin Commands

The following margin commands can be entered on the Profile Index Display panel to perform the function listed against the entity-occurrence on that line. You can use the following margin commands for all entity-types. You can obtain a list of these commands by entering the MARGIN command on any panel.

Use the following margin commands to place maintenance functions in the online work queue:

Margin Command	Equivalent Command
CAT	CATALOG

DEL or DLT	DELETE PROFILE
UPD	UPDATE PROFILE

The following margin commands place specific display functions in the work queue:

Margin Command	Equivalent Command
DDF	DISPLAY DEFINITION PROFILE
DUS	DISPLAY USAGE PROFILE

Executing the Work Queue

You retrieve an entity-occurrence from the queue by entering the PROCESS command or pressing PF4. When an entity-occurrence is retrieved from the queue, it becomes the anchored entity-occurrence and is displayed on the processing panel for the requested function. The entity-occurrence remains anchored until you enter the END, PROCESS, OFF, or OFFON commands.

If you add more entity-occurrences to the work queue during processing of your original set, the new entity-occurrences are added to the top of the queue and are processed first. When you complete processing of the second set of entity-occurrences, processing of entity-occurrences remaining in the original set resumes. When no more entity-occurrences exist in the queue, a message is displayed.

Profile Maintenance Panel Error Codes

The following error codes are presented on the UPDATE PROFILE Panel if an error is encountered. The error code is displayed when you apply the maintenance. You also receive an error message in the format *DDOL000nnn*.

Note: For the error message, see the *CA Datacom/DB Message Reference Guide*.

Code	Problem
A	Invalid function for command
B	Invalid type
C	Unknown entity-type
D	Invalid facility
E	Invalid function (not A)
F	Not found for update or delete
G	Version/Status invalid

H	Facility already related
I	Entity table already related

Signing On to CA Datacom Datadictionary Online

The online facility provides panels for you to enter data to place in CA Datacom Datadictionary. These panels are accessed through the Datadictionary Mode Selection panel (main menu) by selecting option 4 (AUTHORIZE). You must be authorized as a CA Datacom Datadictionary Security Administrator to use this mode.

When you select the AUTHORIZE Mode you receive the following prompter panel where you reenter your password, or change your password.

```
=>
=>
=>

--------------------------------------------------------------------------------

                Authorization Mode Security Check                       T04F

Please re-certify your identity before accessing DD Authorization Mode by
entering your DD User password.

Password:
```

After reentering your password, or specifying a different password, press Enter. If you have the necessary authorization, you receive the following menu to select the desired security maintenance function.

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          P04M
Enter desired option number ===> __    (There are 11 options on the menu)

 1. MAINTAIN PERSON       (MNT PER)     Maintain PERSON definitions
 2. ADD PROFILE           (A PROF)      Add a PROFILE
 3. UPDATE PROFILE        (U PROF)      Update a PROFILE
 4. DELETE PROFILE        (DEL PROF)    Delete a PROFILE
 5. CATALOG PROFILE       (CAT PROF)    Catalog a PROFILE
 6. DISPLAY PERSON        (D PER)       Display PERSON definitions
 7. DISPLAY INDEX PROFILE (D I PROF)    Display a PROFILE Index
 8. DISPLAY USAGE PROFILE (D USE PROF)  Display a PROFILE Usage
 9. DISPLAY DEF PROFILE   (D DEF PROF)  Display a PROFILE definition
10. SET MODE                            Reset DATADICTIONARY processing mode
11. IDEAL                               Transfer to IDEAL application
12. OFF                                 End session
```

Note: If CA Ideal is not installed on your system, the OFF option appears in place of the CA Ideal option.

Use this menu to choose the CA Datacom Datadictionary Security maintenance function by entering the option number or by entering the abbreviated form of the command in the command area and press Enter. For more information and an explanation of the specific options available on this menu, see the appropriate sections in this guide.

Adding CA Datacom Datadictionary Profiles

With the ADD PROFILE function of CA Datacom Datadictionary Security, you can add profiles to CA Datacom Datadictionary either in batch or online.

Use the following steps in CA Datacom Datadictionary online.

Step 1

Select option 2 on the Datadictionary Security Maintenance Menu, or enter the ADD PROFILE command in the command area. For more information and instructions about using this command, see Using Command Processing (see page 119).

If you omit the entity-occurrence name with the command, CA Datacom Datadictionary displays the following panel.

```
=>
=>
=>
1-DDOL000374A - 40FP - REQUIRED PROFILE NAME MISSING
--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
ADD      PROFILE    _________________________________
ADD      PROF       (name)
```

Step 2

Type the profile name as described next and press Enter. CA Datacom Datadictionary displays the panel that follows.

(name)

The name of the profile you are adding. The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
ADD PROFILE $DD-PROGRAMMER                                              T42U

.......................... FACILITY LEVEL SECURITY ..........................
Online Facilities - ( DBM: _    FMM: _    ENTM: _    ENTD: _    ISF: _    SQL: _ )
Batch  Facilities - ( UPD: _    UTL: _     CFB: _     BTG: _    RMF: _    TRS: _ )

........................... ENTITY LEVEL SECURITY ............................
======  =  ================================  ================================
000001  _  AREA
000002  _  AUTHORIZATION
000003  _  CONSTRAINT
000004  _  DATABASE
000005  _  DATAVIEW
000006  _  ELEMENT
000007  _  FIELD
000008  _  FILE
PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS    MORE....
PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

Step 3

Type the relevant information on this panel, described next, and APPLY (PF9) to display the next panel in this series. Use the scroll keys or commands to view all entity-type entries on this panel. For more information, see Profile Maintenance Panel Error Codes (see page 140).

ADD PROFILE

The $DD- Profile entity-occurrence name you added on the Add Profile prompter panel or the profile entity-occurrence name you added with the ADD PROFILE command displays in this field.

Facility Level Security section

Contains all the online and batch facilities available in CA Datacom/DB and CA Datacom Datadictionary. Indicate by typing the letter Y (yes) that authorization to use the following facilities is associated with this profile.

Note: If SQL processing is available at your site, the Interactive SQL Service Facility is securable by entering Y for SQL in this section.

ID	Online Facility
DBM	CA Datacom/DB Structure Maintenance
ENTD	CA Datacom Datadictionary Entity Display
ENTM	CA Datacom Datadictionary Entity Maintenance
FMM	CA FILE Structure Maintenance

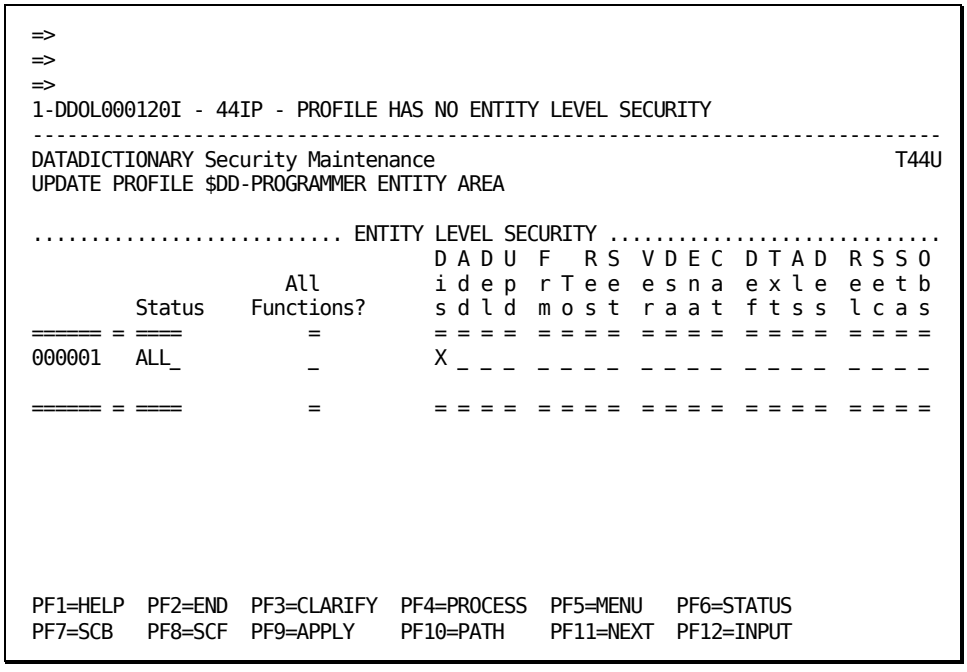
ISF	Interactive Service Facility
SQL	Interactive SQL Service Facility
BTG	DDBTGLM maintenance
CFB	DDCFBLD maintenance
RMF	DDRMFLM maintenance
UPD	DDUPDATE maintenance
UTL	DDUTILTY maintenance

Entity Level Security section

Contains an index of all the valid entity-types for this CA Datacom Datadictionary as determined from the High-Speed Directory (HSD), plus one for UNIVERSAL.

Type a non-blank, non-null character beside the entity-types you want to select for security authorization. You can use the line command area to perform scrolling functions. For more information, see the Using Line Commands (see page 137).

After selecting entity-types for security authorization, issue the APPLY command. CA Datacom Datadictionary displays a panel as follows, to specify entity level security beginning with the first entity-type selected.



Step 4

CA Datacom Datadictionary displays a separate panel for each entity-type selected on the Add Profile panel, allowing you to select the status level and function level of security. The following describes each field on this panel.

To add status/function information, use the line commands to insert, copy, or delete lines. For more information, see Using Line Commands (see page 137).

UPDATE PROFILE

The CA Datacom Datadictionary entity-occurrence name previously added is displayed.

ENTITY

The CA Datacom Datadictionary entity-type selected previously is displayed.

Entity Level Security section

Contains a list of the functions that you can select for authorization associated with this specific profile.

Status

The status you are authorizing with this entity-type.

Valid Entries:

T*nnn* - where *nnn* is 001—999 for Model Structures
TEST - All test statuses
PROD - Production status
ALL - All statuses

Default Value: (No default)

All Functions

Indicate with any character such as the letter Y (yes) that all functions are authorized for this entity-type in this status.

Valid Entries:

Any non-null, non-blank character

Default Value:

(No default)

Specific Functions

Under the following abbreviations, indicate with any character such as the letter Y (yes) or N (no) whether the function is authorized for this entity-type in this status.

Note: The abbreviations for the functions that can be performed against an entity-type are listed vertically on the panel.

Heading	Function
Add	ADD/CREATE
Als	ALIAS maintenance
Ca	CATALOG
Def	DEFINE
Del	DELETE/REMOVE
Des	DESCRIPTOR maintenance
Dis	DISPLAY
Dsa	DISABLE
Ena	ENABLE
Frm	COPY FROM
Obs	OBSOLETE
Rel	RELDEF/TRANSFER
Res	RESTORE
Sec	PASSWORD/LOCK maintenance
Set	SET
Sta	STATUS maintenance
To	COPY TO
Txt	TEXT maintenance
Upd	UPDATE/MODIFY
Ver	VERIFY

Valid Entries:

Any non-null, non-blank character

Default Value:

(No default)

Step 5

Press PF9 or type APPLY in the command area to apply this information to CA Datacom Datadictionary. If an error is encountered, a code is placed in the field following the line number when the maintenance is applied. For more information and the list of codes, see Profile Maintenance Panel Error Codes (see page 140) or press PF1.

After you have completed this process for each entity-type you selected, CA Datacom Datadictionary displays the Security Maintenance Menu with a SUCCESSFUL SEC PROF ADD message. From this menu, CATALOG the profile to CA Datacom Datadictionary by using option 5 or by issuing the CATALOG PROFILE command on the command line. For more information, see Cataloging Profiles (see page 147).

Batch Transactions

Add profiles in a batch environment by submitting the 1011 - 1013 transactions with the -ADD transaction group. The following is an example of batch transactions adding a Profile for $DD-PROGRAMMER that is authorized to access all facilities (1011 transaction), access all areas (1012 transaction), and access all functions (1013 transaction).

For more information and an explanation of these transactions, see the CA Datacom Datadictionary Batch Security Maintenance (see page 172).

```
-ADD PROFILE,$DD-PROGRAMMER
1011 ADD ALL
1012 ADD AREA(ALL)
1013 Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
-END
```

Cataloging Profiles

To complete the security authorization process, you must catalog the profiles you have defined or updated to the CA Datacom Datadictionary High-Speed Directory (HSD).

Note: Profile definitions are read when a user signs on to CA Datacom Datadictionary. If you update and catalog the profile related to your PERSON entity-occurrence or the profile related to a PERSON entity-occurrence of someone currently signed on, the changes are not enforced until you or the person sign off and sign on again.

Use the following procedures to catalog a profile online. You can also catalog all profiles to the HSD by executing the DDCFBLD utility with the -HSD RESET transaction.

Note: For more information, see the *CA Datacom Datadictionary Batch Reference Guide*.

Use the following steps in CA Datacom Datadictionary online:

Step 1

After you have completed all the panels associated with adding a profile (Add Profile and associated Update Profile Entity panels), catalog the profile by selecting option 5 on the Datadictionary Security Maintenance Menu or by typing the CATALOG PROFILE command in the command area. For more information about the CATALOG PROFILE command, see Using Command Processing (see page 119).

If you omit the profile name in the command, CA Datacom Datadictionary displays the following panel:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
CATALOG  PROFILE    _________________________________
CAT      PROF       (name)
```

Step 2

Type the $DD- profile name on this panel as described following and either press PF9 or enter the APPLY command in the command area to update the High-Speed Directory (HSD) with this profile.

(name)

The name of the profile you are cataloging. The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

If you enter the CATALOG PROFILE command and include the profile name, CA Datacom Datadictionary displays the Catalog Profile prompter panel. Issue the APPLY command (PF9) to catalog the profile to the High-Speed Directory (HSD).

Batch Transactions

Use a transaction in the following format in the DDCFBLD utility to update the CA Datacom Datadictionary High-Speed Directory (HSD).

For more information about the transaction, see CA Datacom Datadictionary Batch Security Maintenance (see page 172).

```
-HSD CATALOG,PROFILE,profile-name
```

Deleting Profiles

If you need to delete a profile you have defined to your system, follow these procedures. You can delete profiles using batch and online facilities.

Use the following steps in CA Datacom Datadictionary online:

Step 1

Either select option 4 on the Datadictionary Security Maintenance Menu, or type the DELETE PROFILE command in the command area to display the Delete Profile Prompter panel. For more information, see ADD PROFILE (see page 121).

If you omit the profile name with the command, CA Datacom Datadictionary displays the following panel:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
DELETE   PROFILE   _______________________________
DEL      PROF      (name)
```

Step 2

Type the name of the profile you are deleting as described following.

(name)

The name of the profile you are deleting. The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

Either press PF9 or type APPLY in the command area to process this delete request. CA Datacom Datadictionary responds by returning to the Datadictionary Security Maintenance Menu displaying either a successful or unsuccessful message in the message area.

If you enter the DELETE PROFILE command and include the profile name, CA Datacom Datadictionary responds with the Delete Profile prompter panel with all the information displayed, including a message to APPLY the delete to CA Datacom Datadictionary.

Batch Transactions

Delete profiles in a batch environment by submitting the -DEL transaction.

For more information about these transactions, see CA Datacom Datadictionary Batch Security Maintenance (see page 172).

```
-DEL PROFILE,profile-name
-END
```

Displaying Index of Profiles

CA Datacom Datadictionary Security provides a way for you to display an index of all the CA Datacom Datadictionary Security profiles defined to the system. Use this capability to determine if the profile you need has already been defined to the system, or if you need to define a new one. You can display an index of the CA Datacom Datadictionary Security profiles either in batch or online.

Use the following steps in CA Datacom Datadictionary online:

Step 1

Either select option 7 on the Datadictionary Security Maintenance Menu, or enter the DISPLAY INDEX PROFILE command. For more information about the DISPLAY INDEX PROFILE command, see Using Command Processing (see page 119).

When you press Enter, CA Datacom Datadictionary responds with an index of the profiles defined to the system.

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T47D
       Profile Index
====== ======================== T O P ===================================
000001 $DD-ADM
000002 $DD-COP
000003 $DD-DIS
000004 $DD-PROGRAMMER
000005 $DD-SEC-ADM
000006 $DD-UPD
====== ====================== B O T T O M ================================




PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS
PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

Step 2

You can enter the following margin commands to maintain profile information.

Margin Command	Description
CAT	Catalog a profile
DDF	Display a profile Definition
DEL	Delete a profile
DUS	Display profile Usage
UPD	Update a profile

Batch Transactions

You can run an Index Report of profiles defined to the system in a batch environment by submitting the -RPT INDEX transaction.

```
-RPT INDEX,AUTHORIZATION,$DD-*(PROD)
-END
```

Displaying Person Definitions

You can display the authorizations assigned to any PERSON entity-occurrence in CA Datacom Datadictionary Security online.

Use the following steps in CA Datacom Datadictionary online:

Step 1

Either select option 6 on the Datadictionary Security Maintenance Menu, or type the DISPLAY PERSON command in the command area to display this information. For more information about the DISPLAY PERSON command, see Using Command Processing (see page 119).

If you do not enter the profile name with the DISPLAY PERSON command, or have selected option 6 on the Datadictionary Security Maintenance Menu, CA Datacom Datadictionary displays the following prompter panel:

```
=>
=>
=>
1-DDOL000452A - 40FP - REQUIRED PERSON NAME MISSING
--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
DISPLAY  PERSON     _______________________________
DIS      PER        (name)
```

Step 2

Type the PERSON entity-occurrence name on this panel as described following.

(name)

(Optional) You can limit the definition to a single entity-occurrence by entering the name of the entity-occurrence. Enter ALL to select all entity-occurrences, or use one or more letters and an asterisk (*) to select several entity-occurrences starting with the same initial characters. For example, to display all entity-occurrences with names starting with D, enter D*.

If you leave this field blank, CA Datacom Datadictionary uses ALL as the default and returns all PERSON entity-occurrences.

Valid Entries:

1 to 32 characters
Generic selection
ALL

Default Value:

ALL

When you press Enter, CA Datacom Datadictionary presents a panel similar to the following example. You cannot update the attribute-values on this panel.

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Profile                                          T46D
DISPLAY PERSON: USERNAME                          User-Password: PSWD
 User-ID: UID  Profile: $DD-ADM                          Security Admin.: Y

.......................... FACILITY LEVEL SECURITY ..........................
Online Facilities - ( DBM: Y   FMM: Y   ENTM: Y   ENTD: Y   ISF: Y   SQL: Y )
Batch  Facilities - ( UPD: Y   UTL: Y    CFB: Y    BTG: Y   RMF: Y   TRS: Y )

........................... ENTITY LEVEL SECURITY ...........................
                                D A D U  F   R S  V D E C  D T A D  R S S O
      Entity            All     i d e p  r T e e  e s n a  e x l e  e e t b
             Status  Functions? s d l d  m o s t  r a a t  f t s s  l c a s
====== ======================= T O P ====================================

000001 AREA
               PROD       Y      Y Y Y Y  Y Y Y Y  Y Y Y Y  Y Y Y Y  Y Y Y Y

PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS    MORE....
PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

DISPLAY PERSON:

This is the name of the PERSON entity-occurrence whose profile is being displayed.

User-Password:

The password, if any, assigned to this PERSON entity-occurrence.

User-ID:

This is the user identification for this PERSON entity-occurrence.

Profile:

This is the entity-occurrence name of the related DD AUTHORIZATION entity-occurrence.

Security Admin.:

Indicates with the letter Y (yes) or N (no) if the user represented by this PERSON entity-occurrence is authorized as a CA Datacom Datadictionary Security Administrator (profile $DD-SEC-ADM).

Facility Level Security section

Indicates with the letter Y (yes) or N (no) if authorization to use the following facilities is assigned to this PERSON entity-occurrence.

ID	Online Facility
DBM	CA Datacom/DB Structure Maintenance
ENTD	CA Datacom Datadictionary Entity Display
ENTM	CA Datacom Datadictionary Entity Maintenance
FMM	File Structure Maintenance
ISF	Interactive Service Facility
SQL	Interactive SQL Service Facility
BTG	DDBTGLM maintenance
CFB	DDCFBLD maintenance
RMF	DDRMFLM maintenance
TRS	DDTRSLM maintenance
UPD	DDUPDATE maintenance
UTL	DDUTILTY maintenance

Entity Level Security section

Contains a list of the function authorizations assigned to this PERSON entity-occurrence for specific entity-types in a specific status.

Entity

The entity-type name.

Status

The status of the entity-type.

All Functions?

Indicates with the letter Y (yes) that all functions are authorized for this entity-type in this status.

Indicates with the letter N (no) that the functions are not authorized for this entity-type in this status.

Specific Functions

Under the following abbreviations, indicates with the letter Y (yes) or N (no) if the function is authorized for this entity-type in this status.

Note: The abbreviations for the functions you can perform against an entity-type are listed vertically on the panel.

Heading	Function	Heading	Function
Add	ADD/CREATE	Obs	OBSOLETE
Als	ALIAS maintenance	Rel	RELDEF/TRANSFER
Cat	CATALOG	Res	RESTORE
Def	DEFINE	Sec	PASSWORD/LOCK maintenance
Del	DELETE/REMOVE	Set	SET
Des	DESCRIPTOR maintenance	Sta	STATUS maintenance
Dis	DISPLAY	To	COPY TO
Dsa	DISABLE	Txt	TEXT maintenance
Ena	ENABLE	Upd	UPDATE/MODIFY
Frm	COPY FROM	Ver	VERIFY

Displaying Profile Definitions

You can display profile definitions to see what facility level security and entity level security has been assigned to a specific profile.

Use the following steps in CA Datacom Datadictionary online:

Step 1

Select option 8 on the Datadictionary Security Maintenance Menu, or enter the DISPLAY DEFINITION PROFILE command in the command area. For more information about entering the command, see Using Command Processing (see page 119).

If you omit the profile name with the command, CA Datacom Datadictionary displays the following panel:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
DISPLAY  DEFINITION
DIS      DEF


           PROFILE  _________________________________
           PROF     (name)
```

Step 2

Type the profile name as described following and press Enter.

(name)

The name of the profile whose definition you are displaying. The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

Step 3

CA Datacom Datadictionary displays a Display Definition Profile panel similar to the following:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance                                        T49D
DISPLAY DEFINITION Profile: $DD-PROGRAMMER

.......................... FACILITY LEVEL SECURITY ..........................
Online Facilities - ( DBM:     FMM:     ENTM:     ENTD: Y   ISF:     SQL:   )
Batch  Facilities - ( UPD:     UTL: Y    CFB:      BTG:     RMF:     TRS:   )

........................... ENTITY LEVEL SECURITY ............................
                                D A D U  F   R S  V D E C  D T A D  R S S O
      Entity              All   i d e p  r T e e  e s n a  e x l e  e e t b
             Status   Functions? s d l d  m o s t  r a a t  f t s s  l c a s
====== ======================== T O P ====================================

000001 AREA
               ALL         N      Y N N N  N N N N  N N N N  N N N N  N N N N
000002 DATABASE
               ALL         N      Y N N N  N N N N  N N N N  N N N N  N N N N
PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS    MORE....
PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

If the display is longer than the screen, you can use the scroll commands or PF keys to move backwards and forwards through the display. Another panel to display the additional fields follows the description of the fields on this panel.

Displaying Profile Usage

You can display an index of all the PERSON entity-occurrences related to a specific profile by following these procedures.

Use the following steps in CA Datacom Datadictionary online:

Step 1

Either select option 8 on the Datadictionary Security Maintenance Menu, or enter the DISPLAY USAGE PROFILE command in the command area to display an index of the PERSON entity-occurrences assigned to a specific profile. For more information about issuing the DISPLAY USAGE PROFILE command, see Using Command Processing (see page 119).

If you omit the profile name with the command, CA Datacom Datadictionary displays the following panel:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
DISPLAY  USAGE
DIS      USE


           PROFILE  _______________________________
           PROF     (name)
```

Step 2

Type the profile name as described following and press Enter.

(name)

The name of the profile for whom you are requesting a usage display. The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

CA Datacom Datadictionary displays a Display Profile Usage panel similar to the following:

```
=>
=>
=>
--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
Security Profile: $DD-PROGRAMMER                                          T48D

       Persons with this Security Profile
====== ======================== T O P ===================================
000001 JAMES-DAVIS
====== ====================== B O T T O M ================================
```

Step 3

Scroll forward if there are more PERSON entity-occurrences than can be viewed on your screen.

Batch Transactions

Report on users of specific profiles in a batch environment by submitting the following transactions. For more information about these transactions, see CA Datacom Datadictionary Batch Security Maintenance (see page 172).

```
-DEF PATH,USERS
-DEF TRACE,AUTHORIZATION.PERSON,PER-ATZ-AUTH
-END
-RPT START,AUTHORIZATION,$DD-PROGRAMMER(PROD),USERS
-RPT INDENTED
-END
```

Maintaining Persons

The CA Datacom Datadictionary Security Facility allows you to add, update, and delete PERSON entity-occurrences and assign them to a profile. You can either maintain PERSON entity-occurrences in a batch or online environment.

Use the following steps in CA Datacom Datadictionary online:

Step 1

Display the panel to maintain PERSON entity-occurrence attributes either by selecting option 1 on the Datadictionary Security Maintenance Menu, or by typing the MAINTAIN PERSON command in the command area. For more information about issuing the MAINTAIN PERSON command, see Using Command Processing (see page 119).

CA Datacom Datadictionary displays the following panel:

```
 =>
 =>
 =>

 --------------------------------------------------------------------------------
 DATADICTIONARY Security Maintenance
                                                                          T41U
 ............................. PERSON ATTRIBUTES ..............................

OPTIONAL:Enter Specific Person- ________________________________
        Name                                                      Sec.
         User-Password     ID  Profile                          Admin.
 000001 DATACOM-INSTALL
                              $DD-ADM                              Y
 ====== ================== B O T T O M   ====================================




 PF1=HELP   PF2=END   PF3=CLARIFY   PF4=PROCESS   PF5=MENU    PF6=STATUS
 PF7=SCB    PF8=SCF   PF9=APPLY     PF10=PATH     PF11=NEXT   PF12=INPUT
```

Step 2

You can add and delete PERSON entity-occurrences using line commands to insert lines or delete lines. For more information about these commands, see Using Line Commands (see page 137).

Deleting a line indicates that the PERSON entity-occurrence is to be deleted. Only the PROD version is deleted. Inserting a line indicates that the PERSON entity-occurrence is to be added. When a PERSON entity-occurrence is added, it is immediately updated to PROD status.

Move line commands are not allowed on this panel.

You can also update the User-Password or user ID. When the user ID is updated, not only is the attribute updated, but the previous ALIAS is deleted and a new one is added.

Note: The passwords do not display. To view the passwords, run a Detail Report and specify the override code.

The following list describes each field, the valid entries and the default (if one exists). Fields that require an entry are highlighted on your terminal. Fields which are not highlighted indicate that an entry is optional.

Specific Person-

Use this field to locate a previously defined PERSON entity-occurrence. You can enter the exact name or the beginning letters followed by an * (asterisk) or + (plus sign).

Name

The PERSON entity-occurrence name in PROD status is displayed in this field.

Valid Entries:

1- to 32-character name, blanks, or nulls

Default Value:

(No default)

User-Password

(Optional) The PASSWORD attribute of the PERSON entity-occurrence. Use the EOF key to delete the previous password before entering a new password.

Valid Entries:

1 to 12 characters

Default Value:

(No default)

ID

The user-ID attribute of the PERSON entity-occurrence. When the user ID is updated, not only is the attribute updated, but the previous ALIAS is deleted and a new one is added.

Valid Entries:

3 alphanumeric characters

Default Value:

(No default)

Profile

The name of the profile to which this PERSON entity-occurrence is to be assigned. The profile name must begin with $DD-.

If the profile field is altered, the CA Datacom Datadictionary Security Facility attempts the following:

- If the field was not previously filled in, then the PERSON entity-occurrence is related to the AUTHORIZATION entity-occurrence for the profile.
- If the field contained a profile name that was changed, the PERSON entity-occurrence is first related to the AUTHORIZATION entity-occurrence for the new profile. Only if this is successful is the relationship to the previous AUTHORIZATION entity-occurrence deleted.
- If the field contained a name that was overlayed with blanks or nulls, then the relationship to the previous AUTHORIZATION is deleted.
- If the name specified does not exist, an error message is displayed indicating that the profile does not exist.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

Sec. Admin.

Indicates if the PERSON entity-occurrence is assigned CA Datacom Datadictionary Security Administrator authority with Y (yes) or with N (no).

If the Security Administrator field is altered, the Security Maintenance Facility attempts the following:

- If the field is changed to Y, the PERSON entity-occurrence is related to the $DD-SEC-ADM AUTHORIZATION entity-occurrence.
- If the field was initially Y and is changed to N, the relationship to the $DD-SEC-ADM AUTHORIZATION entity-occurrences is deleted.

  Note: All PERSON and AUTHORIZATION entity-occurrences are added and maintained in PROD status.

Valid Entries:

Y or N

Default Value:

N

Step 3

All maintenance to the CA Datacom Datadictionary database is only performed when the APPLY command (PF9) is issued.

When an error is detected, the panel scrolls to the line in error and a message displays. No subsequent lines are processed until the next APPLY command.

Batch Transactions

Maintain PERSON entity-occurrences in a batch environment by submitting the 1010 transaction with the -ADD and -UPD PERSON transaction group to assign a profile to a PERSON.

If you are adding a PERSON entity-occurrence, include an -UPD PERSON transaction to update the person being added to PROD status.

For more information about the -ADD header and the 1010 and 1014 transactions, see Maintaining and Cataloging Profiles (see page 172). Examples for the transactions follow:

```
-ADD PERSON,JAMES-DAVIS
1010 ADD $DD-PROGRAMMER
1014 JIM          JGD
-UPD PERSON,JAMES-DAVIS(001),PROD
-END
```

Updating Profiles

You can add, update, and delete profile information defined to CA Datacom Datadictionary Security online or in batch. Use the following steps to update profiles:

Note: A profile definition is read when a user signs on to CA Datacom Datadictionary online or when a user identification transaction is processed in batch. When you update and catalog the profile related to your PERSON entity-occurrence or the profile related to a PERSON entity-occurrence of someone currently signed on, the changes are not enforced in online processing until you or the person sign off and sign on again.

Step 1

Display the panel to update profiles either by selecting option 3 on the Datadictionary Security Maintenance Menu, or by typing the UPDATE PROFILE command in the command area. For instructions on using the UPDATE PROFILE command, see Using Command Processing (see page 119).

If you omit the profile name with the command, CA Datacom Datadictionary displays the following panel:

```
=>
=>
=>
--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance
                                                                          T40F
UPDATE   PROFILE     _________________________________
UPD         PROF     (name)


             ENTITY  _________________________________
             ENT     (type)
```

Step 2

Type the profile name to update all levels of CA Datacom Datadictionary Security; also type the entity-type name to *only* update the entity-type level of security for the profile named.

(name)

The name of the profile you are updating. The profile name must begin with $DD-.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

(type)

The entity-type name you are updating, if only updating entity-type level security for the profile named.

Valid Entries:

Valid CA Datacom Datadictionary long name for the entity-type

Default Value:

(No default)

If you only fill in the profile name, CA Datacom Datadictionary displays a panel similar to the following example:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance                                        T43U
UPDATE PROFILE $DD-PROGRAMMER

.......................... FACILITY LEVEL SECURITY ..........................
Online Facilities - ( DBM: _   FMM: _   ENTM: _   ENTD: Y   ISF: _   SQL: _ )
Batch  Facilities - ( UPD: _   UTL: Y   CFB: _   BTG: _   RMF: _   TRS: _ )

........................... ENTITY LEVEL SECURITY ............................
                                 D A D U  F   R S  V D E C  D T A D  R S S O
         Entity        All       i d e p  r T e e  e s n a  e x l e  e e t b
            Status   Functions?  s d l d  m o s t  r a a t  f t s s  l c a s
====== = ======================= T O P  ================================

000001   AREA
              ALL          N       Y N N N  N N N N  N N N N  N N N N  N N N N
000002   DATABASE
              ALL          N       Y N N N  N N N N  N N N N  N N N N  N N N N

PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS    MORE....
PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

Step 3

CA Datacom Datadictionary displays the Update Profile panel which contains two sections. One section lists the Facility Level Security authorizations, and one contains the Entity Level Security authorizations. The Entity Level Security section also includes all the entity-type/status combinations which have been defined to this profile.

If the display is longer than the screen, you can use the scroll commands or PF keys to move backwards and forwards through the display. Another panel to display the additional fields follows the description of the fields on this panel.

The following describes each field, the valid entries, and the default (if one exists). Fields that require an entry are highlighted on your terminal. Fields which are not highlighted indicate that an entry is optional.

UPDATE PROFILE

Displays the name of the profile you entered on either the Update Profile Prompter panel or the name you typed with the UPDATE PROFILE command.

Facility Level Security section

Indicate by typing the letter Y (yes) that authorization to use the facility is associated with this profile. N (no) indicates that authorization to use the facility is *not* associated with this profile.

Note: If SQL processing is available at your site, the Interactive SQL Service Facility is securable by entering Y for SQL in this section.

ID	Online Facility
DBM	CA Datacom/DB Structure Maintenance
ENTM	CA Datacom Datadictionary Entity Maintenance
ENTD	CA Datacom Datadictionary Entity Display
FMM	CA FILE Structure Maintenance
ISF	Interactive Service Facility
SQL	Interactive SQL Service Facility
BTG	DDBTGLM maintenance
CFB	DDCFBLD maintenance
RMF	DDRMFLM maintenance
TRS	DDTRSLM maintenance
UPD	DDUPDATE maintenance
UTL	DDUTILTY maintenance

Entity Level Security section

Contains a list of the function authorizations associated with this profile for specific entity-types in a specific status.

Entity

Displays the entity-type names previously defined. To add a new entity-type/status, use the line command to insert lines or to repeat lines and change the name to the entity-type you want to define. Also use the line commands D or DD to delete an entity-type/status. For instructions on using line commands, see Using Line Commands (see page 137).

Valid Entries:

Valid CA Datacom Datadictionary long name for the entity-type

Default Value:

(No default)

Status

Displays the status authorized with this entity-type entity-occurrence. To update the status, type over the previous status entry. To add or delete the status, see the previous discussion on Entity.

Valid Entries:

Tnnn - Where nnn is 001—999
TEST - All test statuses
PROD - Production status
ALL - All statuses

Default Value:

(No default)

All Functions?

Indicate with the letter Y (yes) or N (no) if all functions are authorized for this entity-type in this status.

Valid Entries:

N or Y

Default Value:

N

Specific Functions

Under the following abbreviations, indicate with the letter Y (yes) or N (no) if the function is authorized for this entity-type in this status.

Note: The abbreviations for the functions that can be performed against an entity-type are listed vertically on the panel.

Heading	Function	Heading	Function
Add	ADD/CREATE	Obs	OBSOLETE
Als	ALIAS maintenance	Rel	RELDEF/TRANSFER
Cat	CATALOG	Res	RESTORE
Def	DEFINE	Sec	PASSWORD/LOCK maintenance
Del	DELETE/REMOVE	Set	SET
Des	DESCRIPTOR maintenance	Sta	STATUS maintenance
Dis	DISPLAY	To	COPY TO
Dsa	DISABLE	Txt	TEXT maintenance
Ena	ENABLE	Upd	UPDATE/MODIFY
Frm	COPY FROM	Ver	VERIFY

Valid Entries:

N or Y

Default Value:

N

Step 4

Press PF9 or type APPLY in the command area to apply this information to CA Datacom Datadictionary. If an error is encountered, a code is placed in the field following the line number when the maintenance is applied. For the list of codes, see Profile Maintenance Panel Error Codes (see page 140) or press PF1.

After you have completed this process, CATALOG the profile to the CA Datacom Datadictionary High-Speed Directory (HSD). For more information, see Cataloging Profiles (see page 147).

Updating Profile Entity-Types

Step 1

Display the Update Profile Entity panel by either selecting option 3 on the Datadictionary Security Maintenance Menu and filling in the profile name and entity-type name on the prompter panel displayed, or type the UPDATE PROFILE command in the command area and include the profile *and* the entity-type names. For instructions on issuing the UPDATE PROFILE command, see Using Command Processing (see page 119).

If you use either method, CA Datacom Datadictionary displays the following Update Profile Entity panel:

```
=>
=>
=>

--------------------------------------------------------------------------------
DATADICTIONARY Security Maintenance                                       T44U
UPDATE PROFILE $DD-PROGRAMMER ENTITY AREA

........................... ENTITY LEVEL SECURITY ............................
                                D A D U  F   R S  V D E C  D T A D  R S S O
                     All        i d e p  r T e e  e s n a  e x l e  e e t b
        Status    Functions?    s d l d  m o s t  r a a t  f t s s  l c a s
====== = ====          =        = = = =  = = = =  = = = =  = = = =  = = = =
000001   ALL_          _        Y N N N  N N N N  N N N N  N N N N  N N N N
====== = ====          =        = = = =  = = = =  = = = =  = = = =  = = = =









PF1=HELP  PF2=END  PF3=CLARIFY  PF4=PROCESS  PF5=MENU   PF6=STATUS
PF7=SCB   PF8=SCF  PF9=APPLY    PF10=PATH    PF11=NEXT  PF12=INPUT
```

Step 2

Update the Entity Level Security on the panel as described following.

If an error is encountered, a code is placed in the field following the line number when you apply the maintenance. For the list of codes, see Profile Maintenance Panel Error Codes (see page 140) or press PF1.

UPDATE PROFILE

The CA Datacom Datadictionary entity-occurrence name previously added is displayed.

ENTITY

The CA Datacom Datadictionary entity-type selected previously is displayed.

Entity Level Security section

Contains a list of the functions which you can change for authorization associated with this specific profile entity-occurrence. To update the fields in this section, type over the information you want to change. To add or delete status/function information, use the line commands to insert, copy, or delete lines. For more information, see Using Line Commands (see page 137). You cannot use the move line commands on this panel.

Status

The status authorized with this entity-type.

Valid Entries:

Tnnn - where nnn is 001—999
TEST - All test statuses
PROD - Production status
ALL - All statuses

Default Value:

(No default)

All Functions?

Indicate with the letter Y (yes) if all functions are authorized for this entity-type in this status. Use N (no) to indicate that they are not.

Valid Entries:

N or Y

Default Value:

(No default)

Specific Functions

Under the following abbreviations, indicate with the letter Y (yes) or N (no) if the function is authorized for this entity-type in this status.

Note: The abbreviations for the functions that can be performed against an entity-type are listed vertically on the panel.

Heading	Function
Add	ADD/CREATE
Als	ALIAS maintenance
Cat	CATALOG
Def	DEFINE
Del	DELETE/REMOVE
Des	DESCRIPTOR maintenance

Dis	DISPLAY
Dsa	DISABLE
Ena	ENABLE
Frm	COPY FROM
Obs	OBSOLETE
Rel	RELDEF/TRANSFER
Res	RESTORE
Sec	PASSWORD/LOCK maintenance
Set	SET
Sta	STATUS maintenance
To	COPY TO
Tx	TEXT maintenance
Upd	UPDATE/MODIFY
Ver	VERIFY

Valid Entries:

N or Y

Default Value:

(No default)

Step 3

Press PF9 or type APPLY in the command area to apply this information to CA Datacom Datadictionary. If an error is encountered, a code is placed in the field following the line number when the maintenance is applied. For the list of codes, see Profile Maintenance Panel Error Codes (see page 140) or press PF1.

After you have completed this process, CATALOG the profile to CA Datacom Datadictionary. For more information, see Cataloging Profiles (see page 147).

Batch Transactions

You can update profiles in a batch environment by submitting any one of the 1011 to 1013 transactions with the -UPD transaction group. The 1011 transaction updates facility level security, the 1012 transaction updates entity-type level security, and the 1013 transaction updates function level security.

For an explanation of these transactions, see CA Datacom Datadictionary Batch Security Maintenance (see page 172).

```
-UPD PROFILE,$DD-PROGRAMMER
1011 DEL DDCFBLD
1012 UPD AREA(PROD)
1013   Y
-END
```

Note: Before you can update a specific status, as shown in this example, the status must have been previously added to the profile.

CA Datacom Datadictionary Batch Security Maintenance

Security Maintenance in batch is performed using DDUPDATE to maintain PERSON and profiles (AUTHORIZATION entity-occurrences) and DDCFBLD to catalog the profiles to the High-Speed Directory (HSD).

Note: For more information about DDUPDATE and DDCFBLD, see the *CA Datacom Datadictionary Batch Reference Guide*.

The -USR transaction used to sign on to the batch facility must also be defined as a PERSON entity-occurrence with security administration authorization ($DD-SEC-ADM).

Maintaining and Cataloging Profiles

To maintain and catalog profiles, use the appropriate header transaction followed by the specific transactions to update CA Datacom Datadictionary Security.

Note: A profile definition is read when a user signs on to CA Datacom Datadictionary online or when a user identification transaction is processed in batch. When you update and catalog the profile related to your PERSON entity-occurrence or the profile related to a PERSON entity-occurrence of someone currently signed on, the changes are not enforced in online processing until you or the person sign off and sign on again.

Header Transactions

The header transactions to maintain profiles in DDUPDATE have the following format. There is no provision for the status/version, password, or override code because profiles are maintained in PROD status and no passwords or lock level settings are allowed.

```
-xxx PROFILE,name
```

-xxx

Is one of the functions being maintained.

Valid Entries:

-ADD - Add a new profile
-UPD - Update an existing profile
-DEL - Delete an existing profile

Default Value:

(No default)

,name

The AUTHORIZATION entity-occurrence name of the profile you are maintaining or cataloging. The name must begin with $DD.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

-ADD and -UPD Transactions

The -ADD and -UPD transactions can be followed by one or more of the following numbered transactions:

1010

Assign or unassign a profile to a PERSON entity-occurrence.

1011

Assign or update a facility to a profile.

1012

Assign or unassign an entity-type to a profile and establish an authorized status if any.

1013

Assign or unassign a function that can be performed against a given entity-type/status in the profile.

The formats of each transaction are as follows:

1010 Transaction

```
1010 xxx occurrence-name
```

xxx

Is the function to perform.

Valid Entries:

ADD
DEL

Default Value:

(No default)

occurrence-name

Is the PERSON entity-occurrence to which the profile is to be related or unrelated using the PER-ATZ-AUTH relationship. The PERSON entity-occurrence must be in PROD status.

Valid Entries:

1 to 32 characters

Default Value:

(No default)

1011 Transaction

```
1011 xxx facility-name
```

xxx

Is the function to perform.

Valid Entries:

ADD
DEL

Default Value:

(No default)

facility-name

Is the name of the CA Datacom Datadictionary facility to assign to the profile.

Note: If SQL processing is available at your site, the Interactive SQL Service Facility is securable by entering Y for SQL in this section.

Valid Entries:

DBMAINT
DDBTGLM
DDCFBLD
DDRMFLM
DDTRSLM
DDUPDATE
DDUTILTY
ENTDISPL
ENTMAINT
FILEMAINT
ISF
SQL
ALL - All facilities are assigned to the profile

Default Value:

(No default)

1012 Transaction

```
1012 xxx entity-type(stat)
```

xxx

Is the function to perform. ADD assigns an entity-type to a profile. UPD alters the functions allowed against an entity-type. It is used with the 1013 transaction. DEL unassigns an entity-type from a profile.

Valid Entries:

ADD
UPD
DEL

Default Value:

(No default)

entity-type

Is the name of the entity-type to be assigned, unassigned, or for which the functions are altered.

Valid Entries:

1- to 32-character entity-type name

Default Value:

(No default)

(stat)

Is the STATUS in which the assigned entity-type and functions (specified by the 1013 transaction) are allowed.

Valid Entries:

Tnnn - where nnn is 001—999
TEST - All test statuses
PROD - Production status
ALL - All statuses

Default Value:

ALL

1013 Transaction

```
1013 function-flags
```

function-flags

Is a series of 20 one-byte flags which indicate if the function is to be allowed with a Y (yes) or N (no). The entity-type and status combination are specified on the previous 1012 transaction.

If neither Y nor N is specified and the 1012 function is UPD, then the flag is not changed. Each flag is separated from the others by a 1-byte filler. The position of each of the flags is:

Position	Function
6	DISPLAY/RETRIEVE
8	ADD/CREATE
10	DELETE/REMOVE
12	UPDATE/MODIFY
14	COPY from
16	COPY to
18	RESTORE

20	SET
22	VERIFY
24	DISABLE
26	ENABLE
28	CATALOG
30	DEFINE
32	TEXT maintenance
34	ALIAS maintenance
36	DESCRIPTOR maintenance
38	RELATE/TRANSFER maintenance
40	PASSWORD/LOCK maintenance
42	STATUS
44	OBSOLETE

Valid Entries:

Y or N

Default Value:

N

-HSD Transaction

The transaction used in the DDCFBLD utility to update the High-Speed Directory (HSD) with a profile entry has the following format. To update the HSD for all profiles, you can execute the DDCFBLD Utility with the -HSD RESET transaction.

Note: For more information, see the *CA Datacom Datadictionary Batch Reference Guide*.

```
-HSD CATALOG,PROFILE,occurrence-name
```

,occurrence-name

Is the name of the AUTHORIZATION entity-occurrence to catalog. ALL specifies that all CA Datacom Datadictionary profiles are to be cataloged. The profile name must begin with $DD.

Valid Entries:

1 to 32 characters
ALL

Default Value:

(No default)

Maintaining Persons

The Security Administrator can add and delete profiles for a PERSON entity-occurrence in either TEST or PROD status. The Security Administrator can also add, delete, or update the PASS-WORD and USERID attributes of a PERSON entity-occurrence in TEST or PROD status.

Profiles, passwords, and user IDs can be maintained for a PERSON entity-occurrence in TEST status, but they cannot be used in the -USR transaction or to sign on to CA Datacom Datadictionary online. To use the PERSON entity-occurrence in this manner, you must update the entity-occurrence to PROD status.

To assign or unassign profiles, use the 1010 transaction. To add additional PERSON entity-occurrences with Security Administrator authorization, use the 1010 transaction to assign a profile $DD-SEC-ADM to those PERSON entity-occurrences.

1010 Transaction

```
1010 xxx profile
```

xxx

Is the function to perform. ADD assigns the profile to the PERSON entity-occurrence. DEL unassigns the profile.

Valid Entries:

ADD
DEL

Default Value:

(No default)

If a PERSON entity-occurrence is already related to a user-defined profile, the existing profile must be deleted before the new profile is added. The following illustrates these transactions:

```
-UPD PERSON,test person-occ(PROD)
1010 DEL $DD-OLD-PROFILE
1010 ADD $DD-NEW
-END
```

1014 Transaction

To add, delete or update the password or user ID, use the 1014 transaction.

```
1014 password     userid
```

password

You must provide this password to access CA Datacom Datadictionary.

Valid Entries:

1- to 12-character user password

Default Value:

(No default)

userid

Code a user ID which must be unique for all PERSON entity-occurrences in CA Datacom Datadictionary. The user can enter the USERID instead of the PERSON entity-occurrence to sign on to CA Datacom Datadictionary. Code this parameter beginning in column 19.

Valid Entries:

Unique 3-character ID

Default Value:

(No default)

The following example illustrates a 1014 transaction:

```
-UPD PERSON,TEST-PERSON(PROD)
1014 TEST-PASSWRD TP3
-END
```

This user could then sign on to batch CA Datacom Datadictionary with either of the following -USR transactions:

```
-USR TEST-PERSON,TEST-PASSWRD

-USR TP3,TEST-PASSWRD
```

Producing a Security Report

You can use the reporting facilities of the DDUTILTY or DDUPDATE utilities to produce reports that display the security structure of CA Datacom Datadictionary. By merging report requests, you can display the PERSON entity-occurrences and determine what access each user has to the CA Datacom Datadictionary.

Note: For more information about producing reports, see the *CA Datacom Datadictionary Batch Reference Guide*.

The first set of example transactions defines a simple path named SECURITY with the relationships discussed previously in this part of the guide from the PERSON entity-type to the AUTHORIZATION entity-type. This is all that is required to generate a useful security report.

The next set of transactions actually defines the report types that are merged to generate the security report.

-RPT START

Defines the PERSON entity-occurrence that is to be the focus of this report. In the following example, the person is D-B-ANALYST.

-RPT INDENT

Indicates that, for every PERSON entity-occurrence accessed, a line in the Indented Report format is generated. This transaction actually would be used when you do not specify a specific PERSON entity-occurrence.

-RPT RELAT

Requests that for every occurrence of the AUTHORIZATION entity-type access, a Relationship Report is generated showing the relationships between the AUTHORIZATION entity-occurrence and any TABLE or SYSTEM entity-occurrences to which it is related. The override code is required to display the user-defined profiles.

The following are the sample batch transactions used to generate the example report through the DDUPDATE or DDUTILTY utility. Since this is a user-defined profile, the override code is required. The four asterisks in the -RPT RELAT transaction represent the override code defined for the CA Datacom Datadictionary.

```
-DEF PATH,SECURITY
-DEF TRACE,PERSON.AUTHORIZATION,PER-ATZ-AUTH
-END
-RPT START,PERSON,D-B-ANALYST(PROD),SECURITY
-RPT INDEN,PERSON
-RPT RELAT,AUTHORIZATION(,****),TABLE,SYSTEM
-END
```

Sample Output - CA Datacom Datadictionary Reports for Security

Following is a sample of the first page of the report. For an example of the report header (not shown here), see Sample Report Headers (see page 16).

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

              *-------------------------------------------------------------------------------*
              *  CODE USER-NAME,PSWD,DATABASE-ID                                              *
              *  -USR SAMPLE-USER,*******                                          ;00PROC    *
              *-------------------------------------------------------------------------------*
```

CODE USER-NAME,PSWD,DATABASE-ID

The first line within this box contains a description of the information that can be entered for the transaction. The second line is the transaction as it was entered, except the user password is replaced with asterisks. (Note that the database ID was not specified.) Following is a sample of the second page of the report.

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

-DEF PATH,SECURITY
-DEF TRACE,PERSON.AUTHORIZATION,PER-ATZ-AUTH
-END
```

-DEF PATH,SECURITY

The transactions that define a path with a name of SECURITY for the reports are displayed exactly as submitted. Following is a sample of the third page of the report.

```
User: SAMPLE-USER                    ********************************************************      DD Base:     2

-RPT START,PERSON,D-B-ANALYST(PROD),SECURITY
-RPT INDEN,PERSON                  ..........
-RPT RELAT,AUTHORIZATION(,****),TABLE,SYSTEM
-END
```

-RPT START,PERSON

These transactions that generate the reports are displayed exactly as submitted.

Note: For more examples of CA Datacom Datadictionary reports, see the *CA Datacom Datadictionary Batch Reference Guide*.

Sample Output - CA Datacom Datadictionary Reports for Security (Continued)

Following is a sample of the first page of the report.

```
User: SAMPLE-USER                  ********************************************************      DD Base:     2

ENTITY-TYPE.................   OCCURRENCE..................................................... S VERS *DATACOM/DB *
                                  DESCRIPTION.............................                        NAME  ID  USE

PER                            D-B-ANALYST                                                    P 0001

AUTHORIZATION                    $DD-DB-ANALYST                                                   (0001)    PROD

  $DD-ATZ-ENT-005                  TABLE
      AREA                                                    (0005)PROD      OBJ       YES       NO
                                                               DD ENTITY AREA

                                        YYYYNNNYYYYYYYYYYYYN                                          RLT
  $DD-ATZ-ENT-P                    TABLE
      AREA                                                    (0005)PROD      OBJ       YES       NO
                                                               DD ENTITY AREA
                                        YNNNNNNNNNNNNNNNNNN                                           RLT
  $DD-ATZ-ENT-005                  TABLE
      DATABASE                                                (0006)PROD      OBJ       YES       NO
                                                               DD ENTITY DATABASE
                                        YNNNNNNYYYYYYYYYYYYN                                          RLT
  $DD-ATZ-ENT-P                    TABLE
      DATABASE                                                (0006)PROD      OBJ       YES       NO
                                                               DD ENTITY DATABASE
                                        YNNNNNNNNNNNNNNNNNN                                           RLT
```

PER / D-B-ANALYST

The first detail line shows the PERSON (PER) entity-occurrence information. In this example, D-B-ANALYST is the only PERSON entity-occurrence requested. If ALL or a generic selection had been specified, each group of relationship definitions would start with a detail line and groups would be presented in alphabetical order.

AUTHORIZATION

The next line shows the AUTHORIZATION entity-occurrence to which the PERSON entity-occurrence D-B-ANALYST is related.

TABLE

Each set of lines shows that the AUTHORIZATION entity-occurrence is related to a TABLE entity-occurrence that defines an entity-type in the DATA-DICT database and details about the relationship and the entity-occurrence. In the example, $DD-ATZ-ENT-005 indicates that this profile establishes access authority to occurrences of the AREA entity-type in T005 status.

Y / N

The series of Y and N characters is from the relationship Intersection Data. This displays the functions that this profile is authorized to perform on the entity-occurrences of the identified entity-types in the identified status. The functions are in the following order:

Position	Function
1	DISPLAY/RETRIEVE
2	ADD/CREATE
3	DELETE/REMOVE
4	UPDATE
5	COPY FROM
6	COPY TO
7	RESTORE TO
8	SET
9	VERIFY
10	DISABLE
11	ENABLE
12	CATALOG
13	FIELD MAINTENANCE
14	TEXT MAINTENANCE
15	ALIAS MAINTENANCE
16	DESCRIPTOR MAINTENANCE
17	RELATIONSHIP MAINTENANCE
18	SECURITY (PASSWORD/LOCK)
19	STATUS CHANGE
20	OBSOLETE

Example Output - Security Report (Continued)

Following is a continuation of the first page of the report.

```
User: SAMPLE-USER                  ********************************************************      DD Base:     2

ENTITY-TYPE.....................   OCCURRENCE.....................................................   VERSION   STATUS
                                          DESCRIPTION.......................
  RELATIONSHIP NAME..............   ENTITY-TYPE.....................
      OCCURRENCE.....................................................   VERSN/STAT     ROLE     LINKED    ORDERED
                                                                        DESCRIPTION.......................

  $DD-ATZ-ENT-005                   TABLE
      TABLE                                                          (0002)          OBJ       YES       NO

                                          YYYYNNNYYYYYYYYYYYN                                                RLT
  $DD-ATZ-ENT-P                     TABLE
      TABLE                                                          (0002)          OBJ       YES       NO

                                          YNNNNNNNNNNNNNNNNNN                                                RLT

AUTHORIZATION                     $DD-DB-ANALYST                                                        (0001)    PROD
  $DD-ATZ-SYS-SEC                   SYSTEM
      $DD-BAT-BTG                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-BAT-CFB                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-BAT-TRN                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-BAT-UPD                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-BAT-UTL                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-ONL-DBM                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-ONL-ENTD                                                   (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-ONL-ENTM                                                   (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
      $DD-ONL-FMM                                                    (0001)PROD      OBJ       YES       NO
                                                                                                           RLT
                                     *--------  E N D   O F   J O B  -----------*
```

AUTHORIZATION / $DD-DB-ANALYST

At this point, the report begins displaying the relationships between the same AUTHORIZATION entity-occurrence ($DD-DB-ANALYST) and occurrences of the SYSTEM entity-type. These relationships indicate which CA Datacom Datadictionary facilities a user who is assigned this profile can use.

Definition Name	Batch Facility
$DD-BAT-BTG	DDBTGLM maintenance
$DD-BAT-CFB	DDCFBLD maintenance
$DD-BAT-TRN	DDRMFLM maintenance
$DD-BAT-TRS	DDTRSLM maintenance
$DD-BAT-UPD	DDUPDATE maintenance
$DD-BAT-UTL	DDUTILTY maintenance

Definition Name	Onine Facility
$DD-BAT-UTL	DDUTILTY maintenance
$DD-ONL-DBM	CA Datacom/DB Structure Maintenance
$DD-ONL-ENTD	CA Datacom Datadictionary Entity Display
$DD-ONL-ENTM	CA Datacom Datadictionary Entity Maintenance
$DD-ONL-FMM	File Structure Maintenance
$DD-ONL-ISF	Interactive Service Facility
$DD-ONL-SQL	Interactive SQL Service Facility

Chapter 4: DQ Internal Security

This chapter discusses CA Dataquery internal security. Securing CA Dataquery using external security is discussed in Using External Security for CA Datacom.

Understanding CA Dataquery Security Concepts

The intention of this section is to give you an understanding of CA Dataquery Security concepts and a suggested plan for the implementation of those concepts. Read this section thoroughly and use the information to plan for the security of your site. It is important that your security plan ensures the security of the data for your site and the CA Dataquery system and the integrity of your data.

Planning

CA Dataquery permits several levels of use and data access. Therefore, CA Dataquery security requires careful thought and planning involving:

- Your site's data
- The way the data is used
- Who is allowed access to the data
- Who is to administer access to data
- Who is to administer authorization to use CA Dataquery
- Who is to plan and administer CA Dataquery security
- The usage of DQL and SQL modes
- Coordination of security with the site Database Administrator and CA Datacom Datadictionary Administrator and with the CA Dataquery Administrator

Important! CA Datacom/DB database IDs can range from 1 to 5000. However, CA Dataquery internal security only allows three digits for a database ID. Therefore, if you have tables in databases with IDs greater than 999 that need to be secured, you must use external security.

Concepts

Following are some of the tasks discussed on the following pages:

- Understanding CA Dataquery and external security
- Authorizing users to access data
- Securing data access for DQL use

- Limiting access to columns
- Securing data access for SQL use
- Miscellaneous security control techniques
- Considering CA Datacom system security

CA Suggests

After your plan has been in effect for some time, you might need to make changes to your original plan. CA Dataquery is flexible and allows you to make changes easily. We suggest that you reread this document before making changes, to ensure that the changes are consistent with the concepts discussed here and your site-defined plan.

You can establish security through CA Dataquery and you can choose to use any external security management product, such as CA ACF2 and CA Top Secret, to define your CA Datacom/DB and CA Dataquery access rights. CA Dataquery users must be assigned access to CA Datacom/DB tables through the security in force for CA Datacom/DB before they can access tables using CA Dataquery.

CA Dataquery Security

CA Dataquery provides several types of security. You can limit access to:

- CA Dataquery through a signon procedure and/or a signon/off exit
- Data through user authorization
- System functions through user authorization
- Data through group authorization
- Administrative functions through user authorization
- Tables through SECURITY CONTROL
- Rows through restricted conditions
- Columns through CA Datacom Datadictionary profile-codes

You must communicate with the CA Dataquery Security Administrator regarding the CA Datacom/DB and CA Datacom Datadictionary security environment and to determine how security should be implemented for CA Dataquery. You must ensure consistency across the system for security use.

CA Dataquery security must be specified in addition to CA Datacom/DB security unless the CA Dataquery user's definition specifies DATA AUTHORIZED as YES. CA Dataquery security must be specified to use INSERT, UPDATE, or ERASE functions. CA Dataquery Security is used to determine authorization of a user to access data only in DQL Mode.

Securing CA Dataquery Access Through Signon Procedures

You can restrict access to CA Dataquery through a CA Dataquery signon procedure or through a signon/off exit.

Signon Procedure

The CA DataqueryAdministrator creates each user signon. The user signon consists of a user name and an optional password. When the user is created, a PERSON entity-occurrence is automatically added to CA Datacom Datadictionary. To help ensure that your security procedures are simple, and efficient, ensure that the CA Dataquery signon procedures conform to the standards set for the site.

Note: For more information about creating user signons, see the *CA Dataquery Administrator Guide.*

Signon/off Exit

You can use the signon/off exit to interface CA Dataquery with other security packages or to perform your own security checks.

Note: For more information about the signon/off exit, see the *CA Dataquery Administrator Guide*.

User Program Signon

If you want to control access to CA Dataquery by a program written at your site, you can do so.

Note: For more information about initiating CA Dataquery from a program rather than from a terminal, see the *CA Dataquery Administrator Guide*.

Securing Data Access Through User Authorization

The CA Dataquery user authorization consists of authorizing users for specific functions. These functions include:

- Read-only access to all data available to CA Dataquery (DATA AUTHORIZED=Y)
- Query creation and maintenance (ASSOCIATE USER=N)
- Batch query submission (SUBMIT ALLOWED=Y)
- Ability to export data (EXPORT ALLOWED=Y)
- Administrative functions

Note: For more information about user authorization, see the *CA Dataquery Administrator Guide*.

Securing Access to Tables, Rows, Columns, and Queries

CA Dataquery provides several methods to secure access to data. You can limit access to:

- Tables
- Rows and columns
- Queries

Limiting Access to Tables in DQL Mode

The Security Administrator should work with you to list all the CA Datacom/DB tables, rows, and columns that the users will query and to determine which users need access to which tables. The Administrator assigned to the security control function implements the assignment of users to a table or tables to a user. This assignment is stored in the CA Datacom Datadictionary DBID named in the System Option Table DQOPTLST DDDBID= parameter.

Additionally, CA Datacom/DB Security can be used to secure tables. For SQL Mode, you can use the SQL GRANT/REVOKE commands to control security. See the CA Datacom/DB security documentation for more information.

Limiting Access to Rows in DQL Mode

When you need to allow users access to some, but not all, of the rows in a table, you use restricted conditions. When you restrict access by column content, you restrict access to all data within that row. For more information, see Limiting Access to Rows Using Conditions and Restrictions (see page 257).

Limiting Access to Columns in DQL Mode

CA Dataquery provides the Security Administrator with the ability to restrict access to columns through CA Datacom Datadictionary profile-codes. A profile-code is a special attribute of a column entity used to put sensitive columns into categories. You and the Security Administrator should meet to decide what columns should be secured and what the profile-code should be. The profile-code must be included in the column definition in CA Datacom Datadictionary. Only users who are authorized for that profile-code can FIND and/or UPDATE data in the protected columns. For more information, see How to Limit Access to Columns (see page 253).

Limiting Access to Queries in SQL Mode and DQL Mode

The Security Administrator can limit access to queries by assigning the query to a group ID or by defining a query as private. The System Option Table DQOPTLST macro parameter, QRYGRPS=, must be specified as YES so that the Security Administrator can implement the group assignments for queries. For more information, see Limiting Access to Queries (see page 280).

Adding Users

When CA Dataquery is installed for new users, a user named DATACOM-INSTALL is created and placed in the DQU table. The password for DATACOM-INSTALL is NEWUSER. You can use this ID to define each person who is to use CA Dataquery. When you add or modify a user definition, that definition is stored in the User Table (DQU).

Ensure that you know which users have access to administrative functions and have overrides to system defaults since their actions can affect system operation.

CA Dataquery and External Security

External security provides the ability to control and administer user access to CA Datacom products and company data based on the security profiles that exist in CA ACF2 or CA Top Secret. With internal security, product access and data access are controlled with the security systems built into each product. The difference between external and internal security is where the user access authorizations are maintained.

CA Dataquery security protects product functions unique to CA Dataquery. These functions include CA Dataquery online and batch activity. Internal security uses a secondary product signon for each accessor and permits you to define table authorizations in CA Dataquery security. External security uses the external security user identification and validates table access according to the authorizations defined in CA Datacom/DB security. If external security is used, CA Dataquery provides only column level security.

To use external security with CA Dataquery, it is necessary for each CA Dataquery user to sign on to the externally secured monitor (CICS) under which CA Dataquery operates. The monitor must be externally secured so that the monitor signon affects a signon to the external security package. If external security is specified for CA Dataquery without the monitor being externally secured, the user name retrieved by CA Dataquery from the security package may not be correct. In batch, the SIGN/ON card is ignored if external security is present.

If CA Dataquery is not externally secured, it is not necessary to execute the monitor signon to use CA Dataquery. In this case, when a user issues the DQRY transaction, CA Dataquery presents its signon panel (DQZ10) and CA Dataquery internal security is in effect.

Note: If your site is moving from CA Dataquery internal security to external security, make sure that you provide security information, such as IDs and table authorizations, that matches your current system.

The Security Administrator controls whether the CA Datacom products are secured with external security. If external security is selected, internal security authorizations are ignored. No modifications are required to any CA Datacom product to implement external security.

When external security is used, you may omit reading Authorizing Users in CA Dataquery and Securing Data Access for DQL Use (see page 236). Read Limiting Access to Columns (see page 253) for information relating to DQL Mode column security (profile-codes, conditions and restrictions). SQL Mode is always secured by CA Datacom/DB and by external security when it is in effect. If the SQL option is used at your site, you should also read Securing Data Access for SQL Use (see page 278).

Note: PDB and the STORE command use SQL.

Authorizing Users in CA Dataquery

Once the security plan for your site is developed, and the CA Dataquery users are identified, define each CA Dataquery user to CA Dataquery. When you add or modify a user definition, CA Dataquery stores that definition in the User Table (DQU). (If the user table is enabled, you can execute queries against it. Use the table name DATAQUERY-DQU.) You can define or modify a user by using online CA Dataquery. It is a fast, simple and efficient method.

CA Dataquery provides two options on the CA Dataquery Administrative Menu (USERS and PROFILE) for adding and maintaining users.

Obtaining Authorizations

Within the CA Dataquery system exists a System Option Table created by a macro (DQOPTLST) with a number of parameters which define the CA Dataquery system at each customer site (see the *CA Dataquery Administrator* Guide). These parameters define system-wide limits on such things as:

- Terminal idle time before automatic signoff
- Maximum number of rows a query can find
- Space and system limits on processing time per query

Within the environment defined by the System Option Table, the CA Dataquery Administrator classifies people with signons as CA Dataquery Administrators, users, or associate users. Within those classifications, the CA Dataquery Administrator can define what each user is allowed to do, and can override a few of the System Option Table parameters regarding system storage allotments for individual users. Table and field authorizations are handled in other ways. For more information, see Securing Data Access for DQL Use (see page 236) and Limiting Access to Columns.

Within the individual user authorizations set up by the CA Dataquery Administrator, each user can change some personal specifications by accessing and changing the user's User Profile panel. (Associate users can only access their profiles if the System Option Table parameter ASUPPRO= is set to YES.)

The flexibility of User Table Maintenance makes it possible to assign authorizations according to actual work responsibilities. When you authorize a new user as an associate user, that user becomes limited to functions accessible by PF key on the associate user panels. For an associate user, you can only add the following authorizations on the User Table Maintenance panel:

- Data Authorized
- Personal Database (SQL Option required)
- Submit Allowed
- Export Allowed
- EMAIL Allowed (CA eMail+ signon required)
- SQL and DQL Allowed (SQL option required)

To authorize a person as a *user*, do not select Associate User. You can add any or all of the authorizations described in the list.

The only difference between a user and an administrator is that the administrator is a user who has been given one or more of the following authorizations:

- Conditions
- Restrictions
- Printer Control
- JCL Maintenance
- Diagnostics
- Language
- User Maintenance
- Saved Set Maintenance
- Query Library Maintenance
- Security
- Active User Control

External Security

If CA Dataquery is externally secured, all CA Dataquery security functions and user authorizations must be done through the external security package. When an external security package is in effect, user access to databases and tables is controlled by that package. External security overrides CA Dataquery security at the database and table level. For more information about external security, see Using External Security for CA Datacom.

Users Option

You can enter information online with the USERS option to:

- Add, delete, or maintain users
- Authorize users to SQL and DQL Language
- Authorize users for system management tasks
- Control data access
- Override predefined system options (CA Dataquery System Option Table)

Note: For more information about the System Option Table parameters, see the *CA Dataquery Administrator Guide*.

When a user is added with a private SQL authorization specified, such as is required for SQL use, CA Dataquery automatically creates a schema in CA Datacom Datadictionary for the SQL authorization ID. A schema defines the SQL environment of the individual user. Users must have a schema associated with an authorization ID to use SQL. A schema contains all table, view and privilege definitions owned by a given authorization ID. Any definitions created by the user are automatically added to the schema for the authorization ID specified when they creates the SQL object.

Note: A system utility (DQUSERMT) allows you to maintain the user in batch.

Profile Option

The PROFILE option, <PF10> on the Directory of CA Dataquery Users panel, allows the modification of the individual user-defined profile option defaults for the following CA Dataquery functions and actions:

- Online and batch features
- Primary and secondary language selections
- Network printing options
- SQL Mode and DQL Mode selection

CA Dataquery and External Security

If external security is active on the system, CA Dataquery obtains the signon ID of the user from the external security package. Once the signon ID is retrieved, CA Dataquery checks eligibility of the user to sign on to CA Dataquery.

After CA Dataquery determines that a user is eligible for signon, CA Dataquery makes additional resource checks to determine the access of the user to functions from external security. If a DQU record for the user exists, the record is updated with the latest authorizations from external security. If one does not exist, one is created, since the DQU record also contains various profile options maintainable by the individual user.

The authorizations in effect at the beginning of a CA Dataquery session determine the functions appearing on CA Dataquery menus and the commands allowed throughout the CA Dataquery session. When an externally secured function is requested by command or PF key or from a menu, the function is checked to determine if the user is still authorized.

If external security is not in effect, CA Dataquery internal security is in effect.

Internal Overrides

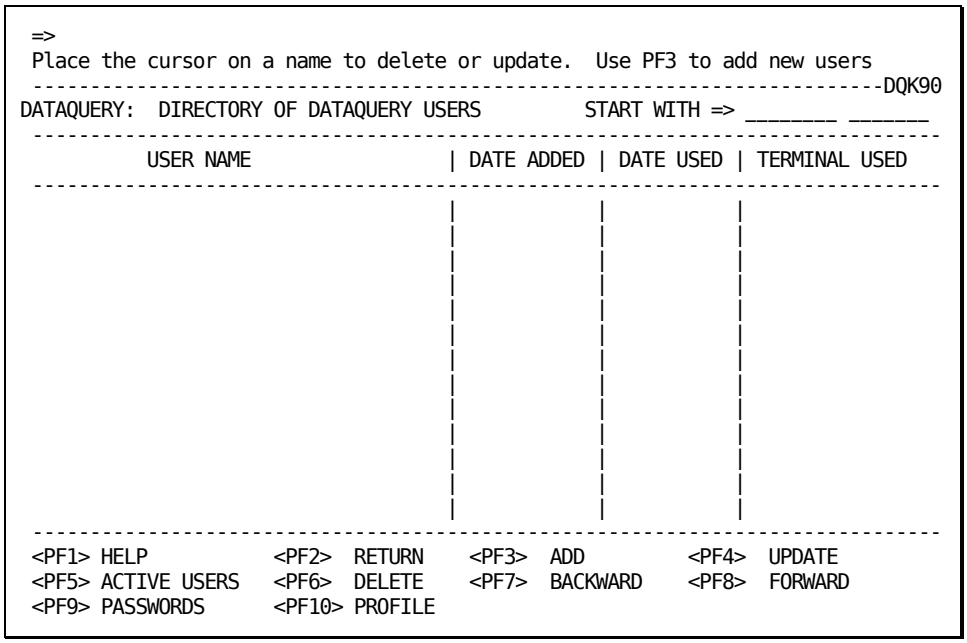
If secured within CA Dataquery, column level security functions, profile codes, and condition/restriction are in effect whether or not CA Dataquery is externally secured.

Implementation of external security in CA Dataquery allows the Security Administrator to define authorizations to perform all CA Dataquery functions and to execute the CA Dataquery batch utility functions using the external security definitions of the user. External security for data (CA Datacom/DB tables) is provided through CA Datacom/DB. When external security is in effect on the system, the signon ID is retrieved from the external security product in both online and batch mode and in the batch utilities.

Accessing User Information

To view, update, add, or maintain users, begin by displaying the Directory of CA Dataquery Users panel (DQK90). Select Users from the Administration menu or type the USERS command and press Enter. A sample panel follows:

Directory of CA Dataquery Users (DQK90)



Action

The START WITH field, located in the upper-right corner of this panel, is where you enter the full or partial name of the user where you want the listing to start. When you press Enter, CA Dataquery displays the user that you specified on the first line of the listing. You can also page forward using <PF8> FORWARD or backward using <PF7> BACKWARD until you reach the member that you want to view and/or edit.

Panel Description

The following list describes each column of the Directory of CA Dataquery Users:

USER NAME

Alphabetical listing of all CA Dataquery user names.

DATE ADDED

Date this user was added to the CA Dataquery system.

DATE USED

Date this user last signed on to CA Dataquery.

TERMINAL USED

Terminal ID from which this user last signed on.

CA Dataquery allows you to invoke several user functions by selecting a PF key. Adding a user is the only PF key selection discussed in this section of this manual. Update, delete, active users, passwords, and profiles are discussed in the following sections of this chapter.

PF Keys

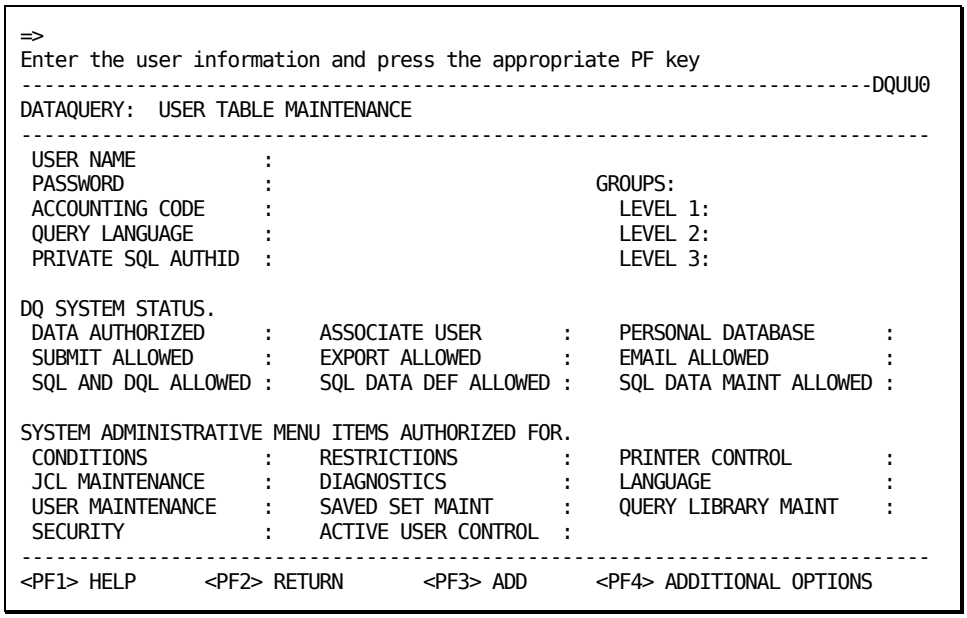
The following list explains unique PF keys for the Directory of CA Dataquery Users panel.

Key	Objective	Result
<PF3> ADD	Add a new user.	CA Dataquery displays User Table Maintenance panel.
<PF4> UPDATE	Modify user options.	CA Dataquery displays User Maintenance panel for user selected by cursor.
<PF5> ACTIVE	Display active users.	CA Dataquery displays Directory of Active Users.
<PF6> DELETE	Delete a user.	CA Dataquery deletes user selected by cursor.
<PF9> PASSWORDS	Modify system and group passwords.	CA Dataquery displays Directory of Defined Dataquery Groups.
<PF10> PROFILE	Display/modify profile of the user.	CA Dataquery displays User Profile for user selected by cursor.

Adding a New User

To add a new user, begin by selecting the USERS option from the Administrative Menu, or typing USERS on the command line and pressing Enter. CA Dataquery then displays the Directory of CA Dataquery Users panel. To add a user, press <PF3> ADD. CA Dataquery displays the User Table as follows. Input the appropriate values for the new user. Each field is explained on the following pages.

User Table Maintenance (DQUU0)



```
=>
Enter the user information and press the appropriate PF key
-------------------------------------------------------------------------------DQUU0
DATAQUERY:  USER TABLE MAINTENANCE
--------------------------------------------------------------------------------
 USER NAME           :
 PASSWORD            :                              GROUPS:
 ACCOUNTING CODE     :                                LEVEL 1:
 QUERY LANGUAGE      :                                LEVEL 2:
 PRIVATE SQL AUTHID  :                                LEVEL 3:

DQ SYSTEM STATUS.
 DATA AUTHORIZED     :    ASSOCIATE USER       :    PERSONAL DATABASE      :
 SUBMIT ALLOWED      :    EXPORT ALLOWED       :    EMAIL ALLOWED          :
 SQL AND DQL ALLOWED :    SQL DATA DEF ALLOWED :    SQL DATA MAINT ALLOWED :

SYSTEM ADMINISTRATIVE MENU ITEMS AUTHORIZED FOR.
 CONDITIONS          :    RESTRICTIONS         :    PRINTER CONTROL        :
 JCL MAINTENANCE     :    DIAGNOSTICS          :    LANGUAGE               :
 USER MAINTENANCE    :    SAVED SET MAINT      :    QUERY LIBRARY MAINT    :
 SECURITY            :    ACTIVE USER CONTROL  :
--------------------------------------------------------------------------------
<PF1> HELP      <PF2> RETURN       <PF3> ADD      <PF4> ADDITIONAL OPTIONS
```

Panel Description

Default values appear on the User Table Maintenance panel and can be changed. Other options relating to overriding system defaults are also available by pressing <PF4> ADDITIONAL OPTIONS. When changes are complete, press <PF3> ADD to add the user.

USER NAME

(Required) Enter a unique 1- to 32-character alphanumeric user name. (The length must not exceed the PERSON entity name length in CA Datacom Datadictionary. See your Security Administrator for this length. Each CA Dataquery user has a matching PERSON entity-occurrence in CA Datacom Datadictionary that is generated automatically by CA Dataquery.)

PASSWORD

(Optional) Enter a 1- to 9-character alphanumeric password. This field is used to assign an individual user password.

ACCOUNTING CODE

(Optional) Specify the CA Datacom/DB accounting code to be used with CA Datacom/DB accounting for CA Dataquery. See your Database Administrator for this information.

QUERY LANGUAGE

(Required) Analyze the language needs of your site. You can authorize use of SQL, DQL Language, or both. Since DQL Mode has security controls that SQL Mode does not offer, and vice versa, ensure that users are authorized for the mode best suited to their job functions and that appropriate CA Datacom/DB security measures are implemented. The CA Dataquery Administrator specifies the query language when they add or update a user and designates if a user can switch between modes. You decide which users are allowed to perform SQL Data Definition statements and Data Maintenance statements, and which statements that the user is authorized to use when adding or updating a user.

SQL if SQL or *DQL*, the default, if DQL Language is authorized for this user. *YES* in the SQL AND DQL ALLOWED field authorizes the user to both query languages.

PRIVATE SQL AUTHID

(Required if language authorized for this user is SQL, or if the user is authorized to use both SQL and DQL Language, or if personal database is authorized for this user.) Enter a 1- to 18-character authorization ID. This is the default authorization ID of the user for personal database and for all SQL Mode. For more information, see the *CA Datacom/DB SQL User Guide*.

Note: If a user changes their SQL authorization ID either by the PROFILE or AUTHID command, it changes only on the user profile, *not* on the User Table Maintenance. Therefore, if a user creates a table in PDB, their private SQL authorization ID is attached to the table name regardless of the authid they were using when they created the table. When the DISPLAY or LIST, EXECUTE or CREATE functions are used, CA Dataquery uses the profile authid.

GROUPS: LEVEL 1

(Optional) Enter a valid 1- to 15-character alphanumeric group level 1 name for CA Dataquery security control. For more information, see Assigning Group Levels (see page 216).

GROUPS: LEVEL 2

(Optional) Enter a valid 1- to 15-character alphanumeric group level 2 name as specified in CA Dataquery security control. If you enter a group level 2 name, you must also enter a group level 1 name. For more information, see Assigning Group Levels (see page 216).

GROUPS: LEVEL 3

(Optional) Specify a valid 1- to 15-character alphanumeric group level 3 name as specified in CA Dataquery security control. If you enter a group level 3 name, you must also enter a group level 1 and a group level 2 name. For more information, see Assigning Group Levels (see page 216).

CA Dataquery System Status

DATA AUTHORIZED

(Required) (Applies to DQL Mode only.) Authorizes the user to read-only access to all data available to CA Dataquery.

Y (yes), you allow the user read-only access to data. CA Dataquery does not perform any data security check. (External security and Database security is applied to table access.)

N (no), the default, CA Dataquery qualifies access to data for this user by the data authorizations specified in security control. However, conditions, restrictions, and profile codes are applied to the appropriate table.

ASSOCIATE USER

(Required) Decide whether to authorize each user as an associate user which limits the ability of the user to query the database. An associate user can only run queries created by others and cannot create or maintain queries. *If you do not designate the user as an associate user, CA Dataquery assigns conventional user authorization to that user.*

Note: A conventional user can create and edit queries.

Y (yes) specifies that this user can only perform associate user tasks.

N (no), the default, does not limit this user to associate user tasks. This enables this user to create and edit queries, view database information, use commands, and so on.

PERSONAL DATABASE

(Required) A user who needs to create tables using the data retrieved by a query for their own use for forecasting is a good candidate for authorization of the Personal database facility. Both DQL Mode and SQL Mode users can be authorized for Personal database, but SQL must be installed at your site to use the Personal database facility. You specify which users can use personal tables and the area of the database where the tables are stored when adding or updating a user in CA Dataquery.

Y (yes) if this user is allowed to create and maintain personal tables using the personal database facility. This authorizes a user to create personal tables within their PRIVATE SQL authorization ID (schema) for their individual use. For more information, see Using Schemas (see page 280) for more information. Specify the area of the database where personal tables are to be stored on the Override System Defaults panel. For more information, see Overriding System Defaults (see page 204).

N (no), the default, prohibits the user from using the personal database facility.

SUBMIT ALLOWED

(Required) Most queries are executed using online CA Dataquery. However, your site can choose to submit long-running queries to batch CA Dataquery to make better use of your system resources. Determine which users need to submit batch queries and authorize them to do so.

Batch CA Dataquery can also be initiated from other software packages. You can secure batch CA Dataquery in this type of environment by using security packages like CA ACF2 and optionally, by use of the Batch Signon Exit.

Indicate whether this user is allowed to submit batch queries from online CA Dataquery.

Y (yes), the default, permits the submission of batch queries

N (no) does not.

EXPORT ALLOWED

(Required) CA Dataquery provides the capability to build a batch export file whereby data accessed from the database is exported and saved on a sequential file for later use. A need of the user for this capability is directly related to their job responsibilities. A data entry clerk most likely does not need to export data to fulfill a customer order. However, a systems programmer might need to export data to test complex queries or to compile statistics. The exported data is in either comma separated value format which is accessed by a personal computer for those users with that specific need or fixed-length record format.

Note: You might want to consider limiting the use of the Export capability.

Y (yes), the default, allows the user to export data. This user is permitted to build a CA Dataquery batch export file whereby data accessed from the database is exported and saved for later use. It allows the user to use the EXPORT command while using batch CA Dataquery.

N (no) prohibits the user from exporting data.

EMAIL ALLOWED

(Optional)

Y (yes) if the user is authorized to send reports to users at your site through CA eMail+.

N (no), the default, prohibits the user from sending reports through CA eMail+.

SQL AND DQL ALLOWED

(Optional)

Y (yes) to allow this user to change query languages on their profile.

N (no), the default, restricts the user from changing to the alternate language and restricts them to one query language.

SQL DATA DEF ALLOWED

(Optional) Consider limiting the use of SQL Data Definition to the CA Dataquery Administrator. This authorization can easily be misused and affect data integrity. Specify N for both SQL Data Definition and SQL Data Maintenance to limit the user to creating only SQL queries using the SELECT statement keywords.

Y (yes) to allow this user to use SQL Data definition statements.

N (no), the default, restricts the user from using CREATE, COMMENT ON, and DROP statements.

SQL DATA MAINT ALLOWED

(Optional) Consider limiting the use of SQL Data Maintenance to the CA Dataquery Administrator. This authorization can easily be misused and affect data integrity. Specify N for both SQL Data Maintenance and SQL Data Definition fields to limit the user to creating only SQL queries using the SELECT statement keywords.

Y (yes) to allow this user to use SQL Data maintenance statements.

N (no), the default, restricts the user from using INSERT, UPDATE, and DELETE.

System Administrative Menu Items Authorized

The following fields allow (or deny) the user access to any or all administrative functions. CA Dataquery automatically gives all users, except associate users, the ability to modify their own profiles. Associate users can do so if the Dataquery System Option Table parameter, ASUPPRO, is set to YES. All fields are required.

CONDITIONS

Y (yes) to allow this user to create, view, delete, or edit a condition.

N (no), the default, restricts this user from the CONDITIONS option on the Administrative Menu.

RESTRICTIONS

Y (yes) if this user is to have the administrative ability to create, delete, view, or edit a restriction.

N (no), the default, denies the user access to the RESTRICTIONS option on the Administrative Menu.

PRINTER CONTROL

Y (yes) permits this user to start, stop, restart, and cancel spooled print jobs.

N (no), the default, restricts access to these spooled print job functions using the PRINTER CONTROL option on the Administrative Menu.

JCL MAINTENANCE

Y (yes) if this user is to create, delete, view, or edit a CA Dataquery JCL member.

N (no), the default, restricts this user from creating, modifying, or deleting a JCL member using the JCL option on the Administrative Menu.

DIAGNOSTICS

Y (yes) to permit this user to request a CA Dataquery Request Table and/or a storage dump in the form of a transaction dump or a module dump.

N (no), the default, restricts the user from requesting a CA Dataquery Request Table or a storage dump through the DIAGNOSTICS option on the Administrative Menu.

LANGUAGE

Y (yes) if the user is to translate, edit, delete, or display CA Dataquery panels, the bulletin board, program literals, and vocabulary terms to another language.

N (no), the default, restricts access to the LANGUAGE option on the Administrative Menu.

USER MAINTENANCE

Y (yes) if this user is to have the administrative function of adding, deleting, and maintaining users, as well as access to active users, passwords, and profiles of other users.

N (no), the default, prohibits this user from viewing and/or accessing the USERS option on the Administrative Menu. If a user is authorized for User Maintenance, that user cannot change his own authorization to *N* (no).

Caution Any user with authorization for this function is able to authorize anyone to perform administrative functions. Take care when deciding who and how many users may have this authority as this is a key to security.

SAVED SET MAINT

Y (yes) to allow the creation, deletion, or modification of a set.

N (no), the default, prohibits access to set definitions using SETS on the Administrative Menu.

QUERY LIBRARY MAINT

Y (yes) if you want this user to create, maintain, execute, and/or submit queries listed on the Admin Directory of Queries and Terms panel.

N (no), the default, does not allow this user to select the LIBRARY option on the Administrative Menu.

SECURITY

Y (yes) if the user is to relate users to a table, tables to a user, or profile codes to a user. This field authorizes this user record and field security control functions.

N (no), the default, restricts this user from performing security control functions.

ACTIVE USER CONTROL

Y (yes), if this user is to have the administrative function of creating and sending messages, forcing another user off CA Dataquery, and cancel query processing during FIND.

N (no), restricts the user from active user administrative functions.

Note: An administrator with user maintenance authority automatically has active user control authority but an administrator with active user control authority only may not add, update, or delete users or passwords, or view other users profiles.

Overriding System Defaults

Summary

Part of the task of adding a new user or modifying a profile of an established user is determining whether that user should be able to override system defaults established by the System Option Table. CA Dataquery allows you to override some predefined system defaults. From the User Table Maintenance panel, select <PF4> ADDITIONAL OPTIONS to display the Override System Defaults panel.

Override System Defaults (DQUM0)

```
=>
Enter the user information and press the appropriate PF key
-------------------------------------------------------------------------------DQUM0
DATAQUERY:  USER TABLE MAINTENANCE - OVERRIDE SYSTEM DEFAULTS
-------------------------------------------------------------------------------
USER NAME        : ________________________________

USER OVERRIDES TO SYSTEM DEFAULTS.
 MXREQ   :             SORTPAG    :         ESTIMATED MAX I/O :
 MXTLR   :             SORTCTG    :
 FNDBLKS :             NETPRT ID  :
 PRIMARY :             SECONDARY  :
 AREA FOR PERSONAL DATABASE TABLES:









-------------------------------------------------------------------------------
<PF1> HELP        <PF2> RETURN        <PF3> ADD           <PF4> NOT USED
```

Action

To override the defaults shown, type over them according to the following information. When the panel is complete, press <PF3> ADD to save the changes. Then press <PF2> RETURN to return to the User Table Maintenance panel.

Panel Description

MXREQ

(Optional. DQL mode only.) A numeric value from 1 through 99999 to specify a search limit for this user that overrides the system default. This feature limits the amount of time CA Dataquery is to process before pausing to allow the user to end the query. MXREQ keeps one query from monopolizing the system. (The system default is used if this value is zeros.)

SORTPAG

(Optional. DQL mode only.) A value from 1 through 1024 to specify, in 4096-byte pages, the maximum amount of storage CA Dataquery is to allocate to process a single sort request without using the database index for sorting. The value specified here overrides the system default for this user.

ESTIMATED MAX I/O

(Optional. DQL mode only.) A value from 1 through 99999 to specify a threshold count of I/O required to process the query. During optimization, if the estimated number of I/Os required to execute the FIND statement exceeds this number, a screen is presented to the user explaining that the MAX I/O has been exceeded, and asking the user if query execution should continue. If not specified, the default value is the value of the MAX I/O parameter from the Dataquery System Option Table.

MXTLR

(Optional. DQL mode only.) A value from 1 through 99999 to specify the number of times CA Dataquery is to relinquish control to other tasks during a query execution before pausing to allow a user to end processing. (The system default is used if this value is zeros.)

The first two features work together, CA Dataquery allows MXREQ to occur MXTLR times before asking the user if they want to terminate the query.

SORTCTG

(Optional) A value from 1 through 16 to specify, in 4096-byte pages, the maximum amount of contiguous storage area for in-core sorting which CA Dataquery requests of CICS at one time. If this amount is not available when needed, CA Dataquery tries to allocate a number of smaller areas for the sort.

FNDBLKS

(Optional) A value from 1 through 99999 to specify the total number of physical blocks on the DQF (online work table) that this user can own at one time during a query execution. Ensure that the value specified for this user still leaves adequate space for all other users. (The system default is used if this value is zeros.)

NETPRT ID

(Optional) Specify the 1- to 4-character network printer ID where reports are to print for this user.

PRIMARY

(Optional) The 2-character primary language ID of the primary language for this user. AE (American English), the default, is automatically distributed with CA Dataquery. Your site can also have German, French, or any other language of your company's choosing for a full or partial translation.

SECONDARY

(Optional) The 2-character secondary language ID for the secondary language of this user. AE (American English), the default, is automatically distributed with CA Dataquery. Your site can also have German, French, or any other language of your company's choosing. (This should be a full translation.)

AREA FOR PERSONAL DATABASE TABLES

(Optional) The 1- to 32-character name for the CA Datacom/DB area used for the personal database tables of this user. This can be used only with CA Datacom extensions to SQL. Check with the Database Administrator for this information.

Updating a User

Choose one of the following to update a user:

- Select the USERS option from the Administrative Menu.
- Type USERS on the command line and press Enter.

When the Directory of CA Dataquery Users panel is displayed, position the cursor on a user name and press <PF4> UPDATE. You can request that the list be positioned on a certain name by entering the command followed by the name of the user.

Example:

```
USER JONES
```

CA Dataquery then displays the User Table Maintenance panel. This panel and all its fields are explained in detail starting in Adding a New User (see page 197). Make any needed changes to the appropriate fields. When you have completed your input, press <PF3> UPDATE to save the new user definition.

Managing Active Users

Summary

You can manage the activities of any user currently signed on to your CA Dataquery system. You are able to:

- Force a user off.
- Send a message to one or more users.
- Cancel any query processing during a FIND.
- Cancel printing for any user.
  (Anyone with PRINTER CONTROL authorization can start, stop, restart, and cancel spooled print jobs using the PRINTER CONTROL option on the Administrative Menu. See Adding a New User (see page 197) to assign printer control.)

Purpose

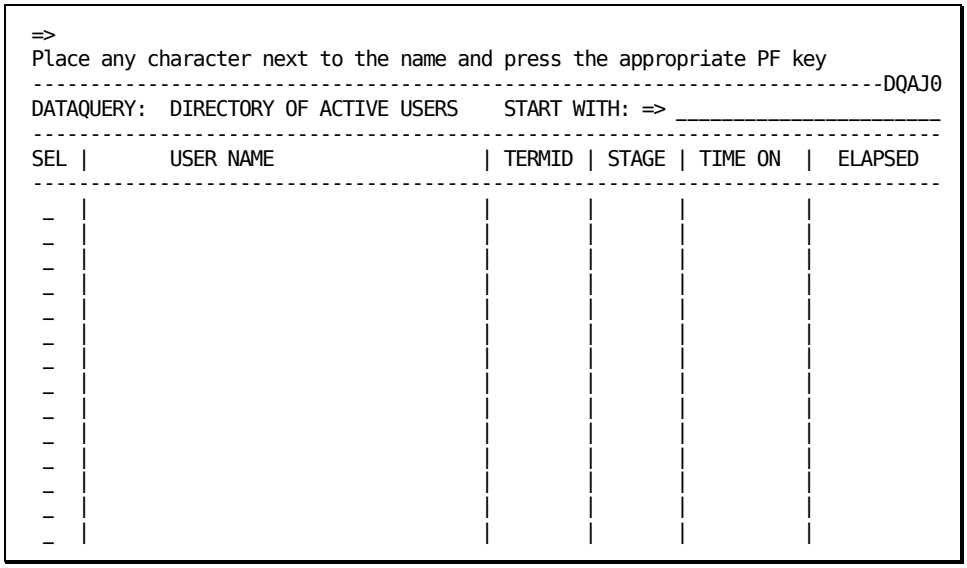
This section describes how to operate the ACTIVE command and tells how to perform these activities.

Choose one of the following to display the active users:

- Select the USERS option from the Administrative Menu, then press <PF5> ACTIVE USERS from the Directory of DATAQUERY USERS panel.
- Type ACTIVE on the command line and press Enter.

CA Dataquery displays the Directory of Active Users panel, allowing you to view the active CA Dataquery users, an example of which follows:

Directory of Active Users (DQAJ0)



Panel Description

Each column on the Directory of Active Users panel is explained in the following list:

SEL

Type any character on the blank to select a user.

USER NAME

Alphabetical listing of all users currently signed on.

TERMID

Terminal ID for the user.

STAGE

Function the user is performing.

ADMIN

The user is performing an ADMINISTRATION function.

DISPL

The user is using a display function (PF keys or commands).

EDIT

The user is on the EDIT panel.

EXEC

The user is executing a query.

FIND

The FIND function is running for an executing DQL query.

GRAPH

The GRAPH function is operating.

GUIDE

The GUIDE function is operating.

HELP

The HELP function is operating.

LIST

A LIST function is operating.

MENU

The user is on the MAIN Menu.

PDB

The user is using the Personal Database Facility.

PERR

An error is being displayed.

SELECT

An executing SQL query is processing the SELECT clause.

SQL

The user is using SQL Mode.

TIME ON

Time this user signed on in hours, minutes, and seconds.

ELAPSED

Amount of time this user has been signed on to CA Dataquery.

Activities

Refer to the following list for instructions on managing active users:

Terminate an active user.

Enter a character next to one or more users' names and press <PF3> FORCE OFF.

Note: We recommend that you warn users by sending a message so they can terminate current processes.

Broadcast a message.

1. Press <PF4> CREATE MSG.
2. Enter a one-line message on the Create a Message panel.
3. Press <PF2> RETURN.
4. Mark users, with any character, to receive the current message.
5. Press <PF5> SEND MSG.

Interrupt query or dialog processing during data selection.

1. Select a user.
2. Check that Stage is Find.
3. Press <PF6> CANCEL FIND.

SQL Mode

The CANCEL FIND function may not be used for an SQL query in the SELECT stage. If long running SQL queries appear to be a problem at your site, contact your Database Administrator for assistance with canceling the long running SQL query and/or reducing the value of the REQTHD parameter of the CA Datacom CICS Services DBCVTPR macro.

The Database Administrator can cancel a long running SQL query in either of two ways:

- Use the COMM function of DBUTLTY to cancel the query's CA Datacom/DB request. The Database Administrator can temporarily reduce the size of the REQTHD parameter of the CA Datacom CICS Services DBCVTPR macro by using the DBOC GENOPTS function. For more information, see the CA Datacom CICS Services documentation.

  Note: For more information, see the *CA Datacom/DB DBUTLTY Reference Guide*.

- Limit the future occurrence of any long running queries (both SQL and DQL) by permanently reducing the size of the REQTHD parameter. This parameter limits the number of CA Datacom/DB requests that any logical unit of work can make. Any tasks exceeding this limitation will abend. For more information, see the CA Datacom CICS Services documentation.

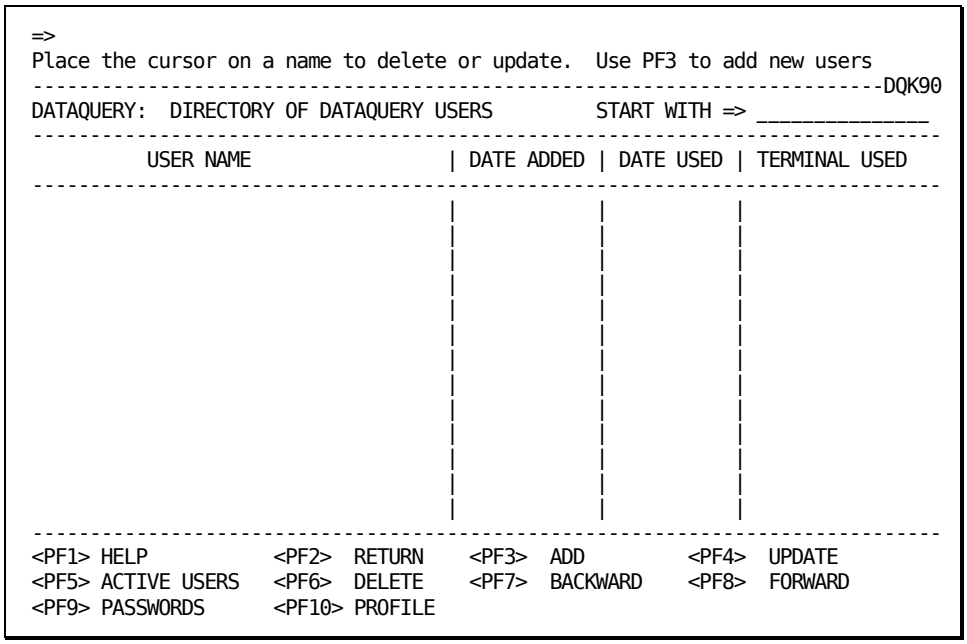
Deleting a User

If you need to delete a user who has left the company or has been transferred, review the queries of the user, terms, dialogs, personal database, and so on, to see if they need to be removed, or assigned to another user.

Important Reassign the JCL members and authorizations that you want to keep before deleting a user because CA Dataquery deletes the user, the JCL member of the user and their authorizations. The CA Datacom Datadictionary PERSON entity-occurrence of the user is not deleted.

An example of a Directory of CA Dataquery Users Panel follows:

Directory of CA Dataquery Users (DQK90)



Action

The START WITH field, located in the upper-right corner of this panel is where you enter the full or partial name of the user where you want the listing to start. When you press Enter, CA Dataquery refreshes the Directory of CA Dataquery USERS panel with the user that you specified on the first line of the listing. You can also page forward using <PF8> FORWARD or backward using <PF7> BACKWARD until you reach the member that you want to view and/or edit.

Choose one of the following to delete the user:

- Choose the USERS option from the Administrative Menu.
- Type USERS on the command line and press Enter.

When CA Dataquery displays the Directory of CA Dataquery Users panel, place the cursor on the user name that you want to delete. (You cannot delete yourself.) Press <PF6> DELETE to delete that user. CA Dataquery then redisplays the Directory of CA Dataquery Users panel.

For an explanation of the Directory of CA Dataquery Users panel and its PF keys, see Adding a New User (see page 197).

Authorizing Administrative Functions

Concept

Because of the impact on security, the number of administrators with User Table Maintenance authorization should be kept to a minimum. You can authorize an administrator for all of the administrative tasks, or you can selectively authorize an administrator for one or more tasks. Evaluate the needs of your site thoroughly before making administrative assignments. CA Dataquery permits you to reassign any of these administrative functions if your needs change.

Administrative Menu (DQKH0)

```
=>

------------------------------------------------------------------------------DQKH0
DATAQUERY:  ADMINISTRATIVE MENU
--------------------------------------------------------------------------------

Enter DESIRED OPTION NUMBER ===>  __

 1.  PROFILE               - Display and update user profile
 2.  CONDITIONS            - List create and maintain conditions
 3.  RESTRICTIONS          - List create and maintain restrictions
 4.  PRINTER CONTROL       - Request control functions for a network printer
 5.  JCL                   - List and maintain batch query JCL
 6.  DIAGNOSTICS           - Produce storage dumps
 7.  LANGUAGE              - Translate DATAQUERY text to another language
 8.  USERS                 - List and maintain DATAQUERY users
 9.  SETS                  - List and maintain saved sets
10.  LIBRARY               - Maintain query library member attributes
11.  SECURITY CONTROL      - Table and column security authorization


--------------------------------------------------------------------------------
<PF1> HELP         <PF2>  RETURN
```

Panel Description

The following is a brief explanation of each administrative function as seen on the panel:

PROFILE

Display or update your profile. CA Dataquery allows each user (who is not an associate user) to modify their profile option defaults for CA Dataquery's online and batch features, primary and secondary language selections, and network printing options. The administrator can modify the profile of any user from the Directory of Dataquery Users panel. Several of the fields in a user profile default to values specified at the time the user is created or maintained using the USERS function discussed next. If you do not specify an option, it defaults to the DQSYSTBL system defaults.

CONDITIONS

Create, delete, view, or edit a condition. A condition (when listed in a restriction) allows a user or group of users access to some, but not all, of the rows in a table based on the content of one or more columns. The administrator names the condition, identifies the table and states the condition. For example, the condition may restrict access to all COMPANY rows containing a value of 20 in the column for sales ID and a value of DALLAS in the city column. You can print a report of each of the conditions with a list of the restrictions where the condition applies. Conditions are discussed in more detail in the section on Using Restricted Conditions (see page 264) in this guide.

RESTRICTIONS

Create, delete, view, or edit a restriction. A restriction is a list of conditions restricting user or group access to view or manipulate data. The administrator can restrict user access at the user level or at the group ID level of the user. Restrictions are discussed in the section on Using Restricted Conditions (see page 264). You can print a report which lists all of the restrictions and the conditions within the restrictions.

PRINTER CONTROL

Display a directory of outstanding network print requests. It allows a request to be canceled (flushed), restarted, or stopped.

JCL

Create, delete, view, or edit JCL members and PROCs. The JCL directory lists the JCL members and PROCs used for executing batch query jobs.

DIAGNOSTICS

Display the CA Dataquery Request Table or request a storage dump in the form of a transaction dump or a module dump. DIAGNOSTICS is used only under the direction of CA Support for the purpose of resolving problems as quickly as possible. The administrator chooses where (terminal ID) and when the dump is turned on or off.

LANGUAGE

Translate, edit, delete, and display CA Dataquery panels, program literals, and vocabulary terms to another language. You can use this function to edit CA Dataquery to reflect a different language, language dialect, or terminology used in your company's daily business. The administrator also uses this function to place messages on the CA Dataquery bulletin board.

USERS

Add, delete, view, and update users, list active users, and send messages. The administrator can maintain name, password, accounting code, group level, and authorization of the user for administrative functions. The administrator can also override system defaults, list and deactivate active users, and send messages.

A CA Dataquery Administrator who is authorized for the USERS function, can establish any new user to CA Dataquery or change signon characteristics of the user as discussed previously. They can also assign system and group passwords. Administrators cannot delete themselves or turn off their USERS maintenance authorization.

The USERS authorization is the key to all other authorizations. Carefully control authorization to this function.

SETS

View, delete, and use all saved found sets. Anyone (except the associate user) who runs a query can save the resulting collection of data as a saved found set. The administrator can reuse the data in a found set, delete the found set, or view a listing of the found sets.

LIBRARY

Create, delete, edit, execute, or submit a query, dialog, or term. The administrator can define or modify the extended definition of a query, dialog, or term which includes specifying it as private or public. They can also modify the groups assigned to the query, dialog, or term and to the author. The administrator can create queries, establish dialog definitions, and submit and validate queries. The LIBRARY function maintains the attributes (extended definitions) of the query library.

If QRYGRPS=YES is specified in the DQOPTLST macro, you can partition the public query library. Once a query, dialog, or term is designated as public, only an administrator with LIBRARY authorization can make changes to it and its extended attributes because queries designated PUBLIC belong to the group not the author. Group level assignments limit the scope of a query, dialog, or term to which the LIBRARY authorization extends. If the group level assignments do not match the administrator's group level assignments, the administrator cannot access the query, dialog, or term. If no group level assignment is made, the access is unlimited.

SECURITY CONTROL

Enables access to data by authorizing DQL Mode users to a database and tables, tables to a user, or profile codes to a user as well as to copy profile codes and authorizations from user to another. This function provides table and column security authorization for a user.

Each of the administrative functions is a tool for the maintenance of your CA Dataquery system. Consider all aspects of your CA Dataquery security as discussed in this chapter before delegating responsibilities. (You can always make reassignments later.) It is useful to assign LIBRARY authorization to one user in each group so that this user can administer public queries, dialogs, and terms for the group. It is imperative that you carefully consider the needs of your site and allocate the authority to use each administrative function to the appropriate user. See Adding a New User (see page 197), specifically the **ASSOCIATE USER** option.

Limiting User Functions to Manipulate Data

CA Dataquery allows you to limit the ability of a user to FIND, UPDATE, INSERT, and ERASE data based on their ability to access that data. Once you have identified all tables, rows, and columns and their related restrictions, decide which functions you permit the user to perform on the accessible data. Users should always be permitted to FIND the data in the authorized tables. However, you probably want to limit the ability of some users to UPDATE, INSERT, and ERASE data. The administrator with SECURITY CONTROL authorization assigns the FIND, UPDATE, INSERT, or ERASE functions when he authorizes each user to a table or profile code in DQL Mode.

Adding and Changing Passwords

Types of Passwords

Passwords can be added or changed on one of three levels:

Individual Password

An individual password is assigned to an individual user to allow access to the CA Dataquery system.

Group Password

A group password is assigned to members of a group.

System Password

A system password protects the CA Dataquery system from unauthorized access from any users who do not use the system password when signing on to CA Dataquery.

Which Password?

Only one of the three types of passwords accesses CA Dataquery. The highest level password is SYSTEM, the next highest level is GROUP and the lowest level password is the individual user password. The highest level password assigned is the only one that accesses the system.

All passwords are one to nine characters in length. The passwords are not displayed at any time. If a user forgets their individual password, assign a new password.

Assigning Passwords to Users and to Groups

Concept

CA Dataquery protects access to the CA Dataquery system on one of three levels, which means that a user can have only one password, individual, group, or system:

- Each individual user can have a unique password to allow access to CA Dataquery, which can be changed as necessary if NEWPASS= YES is specified in the DQOPTLST macro.
- A group can have a unique password to allow users assigned to that group level access to CA Dataquery when they use the group password. The group password supersedes the individual password.
- All users on the system are assigned a common password that allows access to CA Dataquery. The system password supersedes the group and individual passwords.

CA Dataquery protects passwords from indiscriminate viewing by never displaying them. Assigning and changing passwords are the responsibilities of the CA Dataquery Administrator, with user maintenance authorization.

Assigning Group Levels

Concept

A group ID is a defined group of users who are given access to queries, and JCL members (DQL Mode and SQL Mode). The group ID also extends to those users to whom restricted conditions can be assigned (DQL Mode only). Passwords can be assigned by group level.

There are three descending levels of group IDs which can be assigned to a user:

- Level 1 is the high-order group,
- Level 2 is the middle-order group, and
- Level 3 is the low-order group.

If a user is assigned to a level 3 group, the user must also be assigned to a level 2 and a level 1 group. If the user is assigned to a level 2 group, the user must also be assigned to a level 1 group. This group specification limits access of the user to specific data in accordance with the definition established for each group.

For example, if your company were divided into departments called Accounting, Production, Research, and Sales, these categories might be your high-order level 1 groups. If the company were also divided into branches, your middle-order level 2 groups might be Austin, Dallas, Houston, and Midland. Each user could be further categorized according to position for the low-order level 3 groups, for example, Clerical, Executive, Representative, and Supervisor. For instance, a data entry user in Austin could have the following groups:

- Level 1 group: Production
- Level 2 group: Austin
- Level 3 group: Clerical

Groups are a convenient way of organizing and classifying users. Also, you can optionally use groups to partition the public query library and limit users' access to queries. When group level assignments are made to a user or query, those assignments should match, except in the case where the user or query has no group level assignment for one or more levels.

For example, if a user is assigned to group levels as discussed previously and a query is assigned to level 1 - Production, level 2 - Austin, and level 3 - Supervisor, that user could not access this query because the level 3 assignment of the query is Supervisor, not Clerical. However, if the query had no level 3 assignment (it is left blank), users in the Austin production group could access the query.

Under your direction, make group IDs for each user at the time that user is authorized to access CA Dataquery. Group assignments can be modified at any time.

Assigning a Password to a User

Only an authorized administrator can change an individual password. Assign an individual password as follows:

Step 1

Select the USERS option on the Administrative Menu or enter USERS on the command line. Press Enter. CA Dataquery displays the Directory of CA Dataquery Users panel.

Step 2

Place cursor on the name of the user. Press <PF4> UPDATE. CA Dataquery displays the User Table Maintenance panel.

Step 3

Tab over to the PASSWORD field. Enter the password. Press <PF4> UPDATE. CA Dataquery processes the new password which is in effect the next time the user signs on.

Note: The System Option Table parameter NEWPASS= must be YES to allow users to change their individual password on the CA Dataquery signon panel. If NEWPASS= is NO, then only a CA Dataquery Administrator can change individual passwords.

Assigning a Password to a Group or a System

Only an authorized administrator can assign a group or a system password. To assign a group or system password:

Step 1

Select the USERS option on the Administrative Menu, or type USERS on the command line. Press Enter. CA Dataquery displays the Directory of CA Dataquery Users panel.

Step 2

Press <PF9> PASSWORDS. CA Dataquery displays the Directory of Defined Dataquery Groups (DQDB0) panel.

Directory of Defined Dataquery Groups (DQDB0)

```
=>
Place cursor by group assignment and press appropriate PF key.
-------------------------------------------------------------------------------DQDB0
DATAQUERY:  DIRECTORY OF DEFINED DATAQUERY GROUPS  START WITH: _______________
-------------------------------------------------------------------------------
  GROUP LEVEL 1    | GROUP LEVEL 2    | GROUP LEVEL 3    | PASSWORD ASSIGNED
-------------------------------------------------------------------------------
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
                   |                  |                  |
-------------------------------------------------------------------------------
<PF1> HELP         <PF2> RETURN       <PF3> GROUP PSWD   <PF4> SYSTEM PSWD
<PF5> NOT USED     <PF6> DELETE       <PF7> BACKWARD     <PF8> FORWARD
```

This directory is composed of four columns. Each row names the group levels assigned to a user. CA Dataquery specifies a YES or NO in the PASSWORD ASSIGNED column to indicate if a password is assigned for this user. Read the panel to find if any passwords are currently assigned.

Assigning Group Passwords

Assign a group password as follows:

Step 1

On the Directory of Defined Dataquery Groups panel, place the cursor on the group name. Press <PF3> GROUP PSWD.CA Dataquery displays the Password Maintenance - Assign New Password panel.

Password Maintenance - Assign New Password (DQKQ0)

```
 =>
 Enter the new password and press PF3 to assign the password

--------------------------------------------------------------------------------DQKQ0
 DATAQUERY:  PASSWORD MAINTENANCE - ASSIGN NEW PASSWORD

--------------------------------------------------------------------------------


           GROUP LEVEL 1    _______________
                 LEVEL 2    _______________
                 LEVEL 3    _______________

           NEW PASSWORD     _________









 --------------------------------------------------------------------------------
 <PF1> HELP      <PF2> RETURN      <PF3> ASSIGN PASSWORD   <PF4> NOT USED
```

Step 2

Enter the new password in the NEW PASSWORD field. Press <PF3> ASSIGN PASSWORD. CA Dataquery processes the new password which is in effect the next time the user signs on.

Assigning System Passwords

Assign a system password as follows:

Step 1

From the Directory of Defined Dataquery Groups panel, press <PF4> SYSTEM PSWD. CA Dataquery displays the Password Maintenance - Assign New Password panel.

Password Maintenance - Assign New Password (DQKQ0)

```
 =>
 Enter the new password and press PF3 to assign the password
-------------------------------------------------------------------------------DQKQ0
 DATAQUERY:  PASSWORD MAINTENANCE - ASSIGN NEW PASSWORD

--------------------------------------------------------------------------------

           DATAQUERY SYSTEM



           NEW PASSWORD      _________









 --------------------------------------------------------------------------------
 <PF1> HELP       <PF2> RETURN       <PF3> ASSIGN PASSWORD    <PF4> NOT USED
```

Step 2

Enter the new password in the NEW PASSWORD field. Press <PF3> ASSIGN PASSWORD. CA Dataquery processes the new password which is in effect the next time the user signs on.

Deleting Passwords

<PF6> DELETE

Deletes a password for group or system.

Delete an individual password as follows:

Action:

Enter the user's signon and current password. Then, enter **NONE** in the NEW PASSWORD field on the CA Dataquery signon panel. Or, blank the password field on the user maintenance panel.

Result:

Deletes the current password for this user.

Delete a group or system password:

Action:

From the Directory of Defined Dataquery Groups panel, position the cursor on the appropriate line and press <PF6> DELETE.

Result:

Deletes the group or system password.

Performing User Table Maintenance (DQUSERMT)

- Add user authorization
- Update user authorization
- Delete user authorization
- Report by user identifier or group level designation on all or selected users

The CA Dataquery User Table (DQU) stores definitions of valid CA Dataquery users. It contains user attributes (such as name and password) which are used to validate a user. The utility, DQUSERMT, is used to perform the same functions in batch as online. This utility is especially useful for adding a large group of users at one time to the DQU, for example, when CA Dataquery is installed.

Note: If the user table is enabled, you can execute queries against it. Use the table name DATAQUERY-DQU.

User Table Maintenance Control Statements

Use the table maintenance control statements to identify the functions performed by DQUSERMT. A maximum of 60 report and maintenance control statements is allowed. There are five types of maintenance control statements:

SIGN/ON

(Required) Specifies the user ID and password. Only one SIGN/ON statement is allowed and it must be the first statement in the job stream.

ADD

Selects adding a user as the type of maintenance this run performs.

UPDATE

Selects updating a user as the type of maintenance this run performs.

DELETE

Selects deleting a user as the type of maintenance this run performs.

REPORT

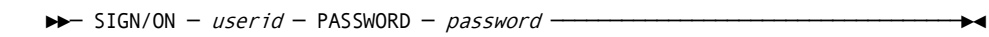
Selects the type of report this run produces.

Enter the control statements in the following sequence.

- SIGN/ON
- ADD, UPDATE, DELETE, or REPORT (use one)

SIGN/ON Statements

For all of the functions the first control statement is the SIGN/ON statement. The SIGN/ON control statement is formatted as follows:



SIGN/ON

(Required) Specifies the user ID and password. Only one SIGN/ON statement is allowed and it must be the first statement in the job stream. The SIGN/ON statement begins in column 1.

userid

Specifies the user ID of the person executing the DQUSERMT utility. The user ID begins in column 11.

Valid Entries:

A 1- to 32-character user ID

Default Value:

(No default)

password

Specifies the password of the person executing the DQUSERMT utility. (PASSWORD keyword is required unless no password is assigned.)

Valid Entries:

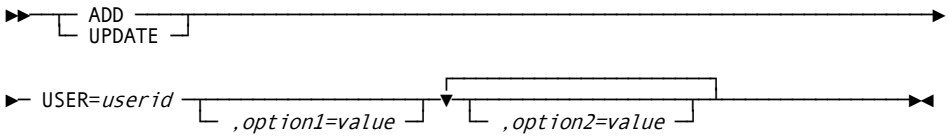
A 1- to 9-character password

Default Value:

(No default)

ADD and UPDATE Statements

For the ADD or UPDATE functions, the second statement in the job stream is ADD or UPDATE.



ADD

To add a new user ID, specify the ADD statement beginning in column 1.

UPDATE

To modify an existing user ID, specify the UPDATE statement beginning in column 1.

USER=

(Required) Beginning in column 11, specify USER= followed by the user ID to add or update.

Valid Entries:

A 1- to 32-character user ID

Default Value:

(No default)

,option1=* and *,option2=

(Optional) Following the user ID, code optional keywords which specify the characteristics of the user ID being added or modified.

The available options are listed in ADD and UPDATE Statement Optional Keywords (see page 225) under the following categories:

- User Authorization Options
- Administrative Functions
- Override System Defaults
- Profile Options
- Printer Options

If you omit an option, CA Dataquery uses the default for that option.

Leave no spaces in the keyword portion of the statement. Use an equal sign (=) to separate an option type from its value, and a comma (,) to separate the options. Do not enter options past column 72. Enter an X (or any non-blank character) in column 72 to indicate that the line is continuing. There are 20 lines allowed for continuations.

ADD and UPDATE Statement Optional Keywords

The COPYFROM= keyword is only valid on an ADD statement. All other keywords are valid on either an ADD or an UPDATE statement.

COPYFROM=

(Optional) Specifies that the characteristics of the new user ID being added are to be copied from an existing user ID. Follow COPYFROM= with an existing user ID. This option can only be used with the ADD statement. This is a very useful option for adding many users.

User Authorization Options

For both the ADD and UPDATE statement, the following options are valid:

ACNTCODE= (Accounting Code)

(Optional) Specify the CA Datacom/DB accounting code to use with CA Datacom/DB accounting for CA Dataquery. See your Database Administrator for this information. (No default)

ASSOCUSR= (Associate User)

(Optional)

Y (yes) specifies that this user can only perform associate user tasks.

N (no), the default, does not limit this user to associate user tasks; thus enabling this user to create and edit queries, view database information, use commands, and so on.

AUSRMNT= (Access User Maintenance)

(Optional)

Y (yes) permits user to see a list of active CA Dataquery users and perform such functions as broadcasting messages, forcing signoff, and cancel FIND in progress.

N (no), the default, does not allow the user to perform active user functions.

DATAAUTH= (Data Authorized)

(Optional) Authorizes the user read-only access to all data available to CA Dataquery.

Y (yes), allows the user read-only access to data. CA Dataquery does not perform any data security check.

N (no), the default, CA Dataquery qualifies this user's access to data by the data authorizations specified in security control.

EMAIL= (CA eMail+ Allowed)

(Optional)

Y (yes) if the user is authorized to send reports to your site's users through CA eMail+.

N (no), the default, prohibits the user from sending reports through CA eMail+.

EXPORT= (Export Allowed)

(Optional) Specify if this user is permitted to build a CA Dataquery batch export file whereby data accessed from the database is exported and saved for later use. It allows the user to use the EXPORT command while using batch CA Dataquery.

Y (yes), the default, allows the user to export data.

N (no) prohibits the user from exporting data.

GROUP1= (GROUP LEVEL 1)

(Optional) Enter a valid 1- to 15-character alphanumeric group level 1 name for CA Dataquery security control. (No default.) For more information, see the discussion in Assigning Group Levels (see page 216).

GROUP2= (GROUP LEVEL 2)

(Optional) Enter a valid 1- to 15-character alphanumeric group level 2 name as specified in CA Dataquery security control. If you enter a group level 2 name, you must also enter a group level 1 name. (No default.) For more information, see the discussion in Assigning Group Levels (see page 216).

GROUP3= (GROUP LEVEL 3)

(Optional) Specify a valid 1- to 15-character alphanumeric group level 3 name as specified in CA Dataquery security control. If you enter a group level 3 name, you must also enter a group level 1 and a group level 2 name. (No default.) For more information, see the discussion in Assigning Group Levels (see page 216).

PASSWORD=

(Optional) Enter a 1- to 9-character alphanumeric password. This field is used to assign an individual user password. (No default.)

QRYLANG= (Query Language)

(Required) Specify SQL if SQL, or DQL if DQL Language, is authorized for this user. DQL is the default and limits the user to DQL Language only. Specifying QRYLANG=SQL and SQLDQL=Y authorizes the user to both query languages. (Default is DQL.) For more information, see ADD and UPDATE Statement Optional Keywords (see page 225).

REPTFAC= (Reporting Facility Allowed)

(Optional)

Y (yes) allows the user to use the CA Dataquery Reporting Facility to produce reports.

N (no), the default, restricts the user from using the CA Dataquery Reporting Facility.

SQLDDEF= (SQL Data Definition Allowed)

(Optional)

Y (yes) to allow this user to use SQL Data definition statements.

N (no), the default, restricts the user from using CREATE, COMMENT ON, GRANT, REVOKE and DROP statements.

SQLDMNT= (SQL Data Maintenance Allowed)

(Optional)

Y (yes) to allow this user to use SQL Data maintenance statements.

N (no), the default, restricts the user from using INSERT, UPDATE, and DELETE.

SQLDQL= (SQL and DQL Allowed)

(Optional)

Y (yes) to allow this user to change query languages on his profile.

N (no), the default, restricts the user from changing from DQL to SQL on his profile. Specifying QRYLANG=SQL and SQLDQL=Y authorizes the user to both query languages. (Default is DQL.) For more information, see ADD and UPDATE Statement Optional Keywords (see page 225).

SUBMIT= (SUBMIT Allowed)

(Required) Indicate whether this user is allowed to submit batch queries.

Y (yes), the default, permits the submission of batch queries.

N (no) does not.

Administrative Functions

The following options enable (or deny) the user access to any or all administrative functions.

COND= (Conditions)

(Required)

Y (yes) if this user is to have the administrative ability to create, view, delete, or edit a condition.

N (no), the default, denies this user access to the CONDITIONS option on the Administrative Menu.

DIAG= (Diagnostics)

(Required)

Y (yes) if this user is to have the administrative ability to request a CA Dataquery Request Table or a storage dump in the form of a transaction dump or a module dump.

N (no), the default, denies the user access to the DIAGNOSTICS option on the Administrative Menu.

FNDSMNT= (Found Set Maintenance)

(Required)

Y (yes) if this user is to have the administrative ability to create, delete, or modify a set.

N (no), the default, denies the user access to the SETS option on the Administrative Menu.

JCLMNT= (JCL Maintenance)

(Required)

Y (yes) if this user is to have the administrative ability to create, delete, view, or edit a CA Dataquery JCL member.

N (no), the default, denies this user access to the JCL MAINTENANCE option on the Administrative Menu.

LANG= (Language)

(Required)

Y (yes) if the user is to have the administrative ability to translate, edit, delete, or display CA Dataquery panels, program literals, and vocabulary terms to another language.

N (no), the default, denies access to the LANGUAGE option on the Administrative Menu.

MAXIO= (Estimated Maximum I/O for a FIND)

(Optional) A value from 1 through 99999 used to specify a threshold value for estimated I/O for DQL find processing. When this value is exceeded, the user is presented a panel and asked if they want to continue. The system default from the CA Dataquery System Option Table is used if this value is zero.

PDB= (Personal Database)

(Required)

Y (yes) if this user is allowed to create and maintain personal tables. Also authorizes a user to create personal tables for his own individual use. Specify the area of the database where personal tables are stored in Override System Options.

N (no), the default, prohibits the user from having personal tables.

PRTCTL= (Printer Control)

(Required)

Y (yes) if this user is to have the administrative ability to start, stop, restart, and cancel spooled print jobs.

N (no), the default, denies the user access to the spooled print job functions on the Administrative Menu.

QRYLMNT= (Query Library Maintenance)

(Required)

Y (yes) if this user is to have the administrative ability to create, maintain, execute, or submit queries listed on the Admin Directory of Queries and Terms panel.

N (no), the default, denies this user access to the LIBRARY option on the Administrative Menu.

REST= (Restrictions)

(Required)

Y (yes) if this user is to have the administrative ability to create, delete, view, or edit a restriction.

N (no), the default, denies the user access to the RESTRICTIONS option on the Administrative Menu.

SECMNT= (Security Maintenance)

(Required)

Y (yes) if the user is to have the administrative ability to relate users to a table, tables to a user, or profile codes to a user. This field authorizes this user record and field security control functions.

N (no), the default, denies the user access to the Security Control option on the Administrative Menu.

USERMNT= (User Maintenance)

(Required)

Y (yes) if this user is to have the administrative function of adding, deleting, and maintaining users, as well as access to active users, passwords, and profile.

N (no), the default, prohibits this user from viewing and/or accessing the USERS and PROFILE options on the Administrative Menu.

Important Any user that has authorization for this function is able to authorize themselves or others to perform any of the administrative functions. Care should be taken when deciding who and how many users may have this authority as this is a key to security. If a user is authorized for User Maintenance, that user cannot change their own authorization to **N** (no).

Override System Defaults

The following options enable the user to override system default options.

AUTHID= (SQL Authorization ID)

(Required if the query language authorized for this user is SQL, or if personal database is authorized for this user, or if SQL AND DQL ALLOWED=YES.) Enter a 1- to 18-character authorization ID. This establishes the default authorization ID of the user for personal database and for all SQL Mode. (No default)

FNDBLKS= (DQF Blocks Available)

(Optional) Enter a value from 1 through 99999 to specify the total number of physical blocks on the DQF (found table) that this user can own at one time during a query execution. Ensure that the value specified for this user still leaves adequate space for all other users. (The system default is used if this value is zeros.)

MXREQ= (Maximum Number of Requests)

(Optional) Input a numeric value from 1 through 99999 to specify a search limit for this user that overrides the system default. This feature limits the amount of time CA Dataquery is to process before pausing to allow the user to end the query. MXREQ keeps one query from monopolizing the system. (The system default is used if this value is zeros.)

MXTLR=

(Optional) Indicate a value from 1 through 99999 to specify the number of times CA Dataquery is to relinquish control to other tasks during a query execution before pausing to allow a user to end processing. (The system default is used if this value is zeros.)

NETPRTID= (Network Printer ID)

(Optional) Specify the 1- to 4-character network printer ID used by this user.

PDBAREA= (Area for Personal Database Tables)

(Optional) Specify the 1- to 32-character name for the CA Datacom/DB area used as personal tables for this user. Check with the CA Datacom/DB Administrator for this information. The default is in the System Option Table or if this is blank, the default is the CA Datacom/DB SQL DEFAULT area specified in Multi-User startup options.

Note: For more information about Multi-User startup options, see the *CA Datacom/DB Database and System Administration Guide.*

PRIMARY= (Primary Language)

(Optional) Specify the 2-character primary language ID for the primary language of this user. AE (American English), the default, is automatically distributed with CA Dataquery. Your site can also have German, French, or any other language that your company chooses. (Default is AE.)

SECONDARY= (Secondary Language)

(Optional) Specify the 2-character secondary language ID for the secondary language of this user. AE (American English), the default, is automatically distributed with CA Dataquery. Your site can also have German, French, or any other language of your company's choosing. (Default is AE.)

SORTCTG= (SORTCTG)

(Optional) Input a value from 1 through 16 to specify, in 4096-byte pages, the maximum amount of contiguous storage area for in-core sorting which CA Dataquery requests of CICS at one time. If this amount is not available when needed, CA Dataquery tries to allocate a number of smaller areas for the sort.

SORTPAG= (SORTPAG)

(Optional) Enter a value from 1 to 1024 to specify, in 4096-byte pages, the maximum amount of storage CA Dataquery is to allocate to process a single sort request without using the database index for sorting. The value specified here overrides the system default for this user. (The system default is used if this value is zeros.)

Profile Options

The following options enable the user to override system default options.

ALIASES= (List and Display Aliases)

(Optional)

Y (yes) to include CA Datacom Datadictionary aliases in the Directory of Tables, Keys and Fields Display, Fields Display, and Keys Display panels.

N (no), the default, excludes CA Datacom Datadictionary aliases from these display panels. (See the CA Dataquery end-user documentation for details on these panels.)

DPCHAR= (Decimal Point Character)

(Optional) Enter 1 character. Specifies the character that the user wishes to use as a decimal point. Do not list as the last option on a statement. If necessary, add the QUERYLANG= option for the mode in use after DPCHAR=. The default is the value of the DECPT= parameter in the System Option Table.

DUPCOLSP= (Suppress Duplicate Columns)

(Optional) Determines if duplicate values for columns specified as control break columns are suppressed in the generated report.

Y (yes), the default, the value contained in a control break column is displayed only once. Each time the value in the control break column changes, the new value is displayed. If the output continues to the top of a new page, the current value in the control break column is displayed at the top of the new page.

N (no), value prints on every detail line.

EXPNLSP= (Suppress Execute Panel)

(Optional)

Y (yes) to suppress the display of the Online Execute Query panel. Users would want to suppress the display of the Online Execute Query panel if their queries always read and collect data and display it on their terminals. Suppressing the display saves a step during the execution process by accepting the execution defaults.

N (no), the default, causes the Online Execute Query panel to display.

GROUPDIS= (Group Display)

(Optional) Determines the manner in which a compound field is represented when displayed on a report.

Y (yes), fields comprising the compound field are shown as individual fields.

N (no), the default, a compound field is shown as though it is a single alphanumeric field, even though one or more of the simple fields contained in the compound field is a numeric field which cannot be printed. (Default is N)

PRTPFKSP= (Suppress PFKeys on Print)

(Optional)

Y (yes) to suppress the PF key descriptions on the print panel that displays the report.

N (no), the default, causes the PF keys descriptions to display.

Printer Options

The valid printer options are:

PBANNER= (Print Banner Page)

(Optional)

Y (yes), the default, if the print jobs of the user are preceded with a banner page containing user name, date, and time, to aid in distributing the reports.

N (no) suppresses the printing of the banner page.

PCOLS= (Printer Number of Columns)

(Optional) Specify the width of the hardcopy on the network printer by stating the number of columns to print. Indicate a 3-character numeric value. Valid entries are 00 or 80 to 255. (Default is 0.)

PPGTOGETHER= (Print Pages Together)

(Optional) Use this field when printing a report composed of two adjacent (side-by-side) pages. If the first page (left-hand page) is labeled A and the second page (right-hand page) is labeled B and the report is three pages in length.

Y (yes), the default, would result in these pages being printed in the order of 1A, 1B, 2A, 2B, 3A, 3B.

N (no) results in a printing order of 1A, 2A, 3A, 1B, 2B, 3B.

PQRYSTAT= (Print Query Statistics)

(Optional)

Y (yes), the default, if the statistics of the query that produced the report are to print when the report is printed on the network printer.

N (no) does not print the query statistics.

PQRYTXT= (Print Query Text)

(Optional)

Y (yes), the default, if the text of the query that produced the report is to be printed when the report is printed on an online network printer.

N (no) does not print the query text.

PROWS= (Printer Number of Rows/Page)

(Optional) Specify the number of rows to print on one page of hardcopy on the network printer. Indicate a 3-character numeric value. Valid entries are 00 or 12 to 255. 1 through 11 are not valid entries. (Default is 0.)

PRTWINDOWS= (Print Using Windows)

(Optional)

Y (yes) if the report extends beyond 80 columns and you do not want the report lines to wrap.

N (No), the default, if you want the print lines to use wrapping.

JCL Examples

Note: Use the following as a guide to prepare your JCL.The JCL statements are for example only. Lowercase letters in a statement indicate a value you must supply. Code all statements to your site and installation standards.

Sample z/OS JCL

```
//jobname    See the note above and page Listing Libraries for CA Datacom Products.
//       EXEC PGM=DQUSERMT
//STEPLIB    See the note above and page Listing Libraries for CA Datacom Products.
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*                          Print Output
//SNAPER   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSIN    DD *
SIGN/ON username PASSWORD password
control statements
/*
//
```

Sample z/VSE JCL

```
* $$ JOB ...        See the note above and Listing Libraries for CA Datacom Products.
* $$ LST ...
// JOB name
// EXEC PROC=procname  Whether you use PROCs or LIBDEFs, see Listing Libraries for
CA Datacom Products.
// EXEC DQUSERMT
SIGN/ON username PASSWORD password
control statements
/*
/&
* $$ EOJ
```

DELETE Statement

The DELETE control statement follows the SIGN/ON statement in the job stream. The DELETE control statement is formatted as follows:

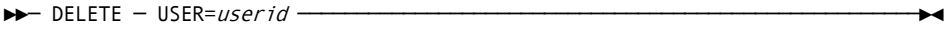
Columns 1-10

Identifies the type of control statement. The valid entry is DELETE. Left-justify the value with trailing blanks as necessary.

Columns 11-72

Specifies the option keyword USER and its value. Enter the user name as the value.

There are no spaces in the keyword portion of the statement. An equal sign (=) separates an option type from its value.



USER=

Specifies the ID of the person todelete from the CA Dataquery system.

Valid Entries:

A 1- to 32-character user ID

Default Value:

(No default)

REPORT Statement

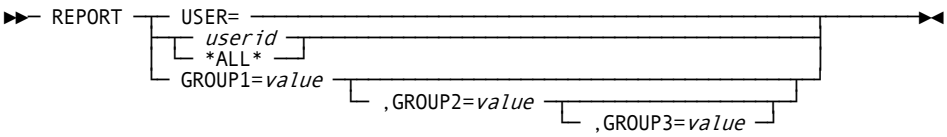
The REPORT control statement follows the SIGN/ON statement in the job stream. The REPORT control statement is formatted as follows:

Columns 1-10

Identifies the type of control statement. The valid entry is REPORT. Left-justify the value with trailing blanks as necessary.

Columns 11-72

Specifies the option keyword and its value, as described next.



USER=

Specifies the user ID of the person whose authorizations are to be reported. To report the authorizations for every user defined to the system, code USER=*ALL*.

Valid Entries:

A 1- to 32-character user ID or *ALL*

Default Value:

(No default)

GROUP1=, GROUP2=, and GROUP3=

Specifies the group ID of the group whose authorizations are to be reported. If you specify GROUP3=, you must also specify GROUP2=. If you specify GROUP2=, you must also specify GROUP1=.

Valid Entries:

A 1- to 32-character group ID

Default Value:

(No default)

Securing Data Access for DQL Use

Securing access to your company's data is a major part of assuring data integrity. If you determined (using the USERS administrative option) that all users are to have unlimited read-only access, they can access all tables, rows, and columns in your database that are not protected by conditions and restrictions. If you do not authorize users for unlimited read-only access, each user can access only those tables (and their rows and columns) that you specifically assign to them.

Summary

This section describes the concepts of assigning users to specific tables, rows, and columns. It also describes how to limit the users' ability to manipulate the data accessed. This section applies only to DQL Mode.

Note: For information about SQL data access, see Securing Data Access for SQL Use (see page 278).

Limiting Access to Database Tables

The Database Administrator can list all CA Datacom/DB tables, rows, and columns that the users are going to query. Determine which users need to access which tables and list each user and the tables to which they need access. If your site security is controlled by an external security package, make sure the Security Administrator who manages that package has this information. CA Dataquery uses the external CA Datacom/DB security for table and database level access.

Table assignments control what each user sees on the Directory of Tables panel. When a list of tables is requested, the current authorization ID of the user is used to read the CA Datacom Datadictionary table for all tables, views, and synonyms for that authorization ID. Items on the list are checked for read(SELECT) authorization by a call to CA Datacom/DB. Although your site might have specified multiple CA Datacom Datadictionary DBIDs, all of the data entered under the SECURITY CONTROL administrative function is stored in the CA Datacom Datadictionary DBID named in the DQOPTLST macro DDDBID= parameter.

When you add a user to CA Dataquery using the User Table Maintenance panel under the USERS administrative function, CA Dataquery automatically creates a CA Datacom Datadictionary PERSON entity-occurrence. This entity-occurrence is added to the dictionary named in the DDDBID= parameter in the DQOPTLST macro. This entity-occurrence name is the same as the CA Dataquery user ID.

For CA Dataquery Security to work there can be no LOCK or password on the following CA Datacom Datadictionary tables:

- Person tables
- Authorization
- Relationship

Personal tables created in DQL Mode cannot be accessed by another user unless the user knows the full name of the table including its AUTHID.

Note: CA Datacom/DB database IDs can range from 1 to 5000. However, CA Dataquery internal security only allows three digits for a database ID. Therefore, if you have tables in databases with IDs greater than 999 that need to be secured, you must use external security.

In SQL Mode, access to personal tables can only be given by the table creator, using the GRANT command or through CA Datacom/DB security. The REVOKE command removes the authorization.

Note: For more information about GRANT and REVOKE, see the *CA Datacom/DB SQL* User *Guide*.

Authorizing Data Access Using the Security Maintenance Menu

Concept

In a secure operating environment, each user is authorized to access only the data necessary to perform their job. Usually, only a select few have a valid need to freely access the database (such as an administrator).

Determine whether you want to allow each user read-only access to all the data in your database through CA Dataquery. CA Dataquery allows you to give users authorization for unlimited read-only access to the database and performs no further table security check on the user when they have this authorization (except restricted conditions in DQL Mode). CA Datacom/DB security or an external security product is always in effect. We suggest you limit this authorization to only a few administrators.

If a user is assigned unlimited read-only access by specifying **Y** (yes) for the DATA AUTHORIZED parameter on the User Table Maintenance panel, that user can access all tables, rows, and columns in your database that are not protected by CA Datacom/DB security, or do not have any restrictions assigned to the user or his groups. This user can also access personal tables of anyone.

If you specify **N** (no) for this field, that user can access only those tables (and their rows and columns) that you specifically assign to that user using the SECURITY CONTROL administrative function. The user can still access other users' personal tables in SQL Mode, if privileges are granted to him.

Regardless of the DATA AUTHORIZED parameter setting, authorize the user, if data is to be modified from DQL Language queries (for INSERT, UPDATE, and ERASE specifically).

How to Limit Access to Tables

Sign on to CA Dataquery and select the SECURITY CONTROL option from the Administrative Menu or enter the SECURITY command on the command line. CA Dataquery then displays the Security Maintenance Menu.

Security Maintenance Menu (DQLA0)

```
=>
-------------------------------------------------------------------------DQLA0
DATAQUERY: SECURITY MAINTENANCE MENU
-------------------------------------------------------------------------

ENTER DESIRED OPTION NUMBER  ___


1.   DATABASE       - Authorize by CA Datacom/DB Bases and Tables to Users
2.   USER           - Authorize by User to CA Datacom/DB Bases and Tables









-------------------------------------------------------------------------
<PF1> HELP     <PF2>  RETURN
```

The CA Dataquery SECURITY CONTROL function provides you with the following options to assign a user to a CA Datacom/DB table:

Panel Description

DATABASE

This option allows you to name the CA Datacom/DB ID and tables that you are allowing a user to access.

For details about using this option, see Naming a CA Datacom/DB Database and Table for User Access (see page 248).

USER

This option allows you to select the user to assign and then select the CA Datacom/DB ID and tables to which this user is allowed to perform the FIND, UPDATE, INSERT, or ERASE commands. You can also copy security from one user to another. These options allow you to specify whether the user can FIND, UPDATE, INSERT, or ERASE the data on that table. We suggest that you authorize users to the FIND function for the tables they require. Without this authorization, the user cannot read the data in the table.

For details about using this option, see Specifying Table Options Using the USER Option (see page 240).

Specifying Table Options Using the USER Option

Access

To authorize a user to perform FIND, UPDATE, INSERT, or ERASE on specific tables, choose the SECURITY CONTROL option from the Administrative Menu. Then select USER from the Security Maintenance Menu. To go directly to the Security User Directory panel, enter SECURITY USER on the command line. (If you must relate many users to many tables, an alternative to online entry exists. See Using CA Datacom Datadictionary to Relate Multiple Users to Tables (see page 252) for details.) CA Dataquery displays the Security User Directory panel.

Security User Directory (DQLM0)

```
=>
 Place the cursor on a name and press the appropriate PF key.
 ------------------------------------------------------------------------------DQLM0
 DATAQUERY:  SECURITY USER DIRECTORY              START WITH => _______________
 ------------------------------------------------------------------------------
           USER NAME                 | DATE ADDED | DATE USED
 ------------------------------------------------------------------------------
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
                                     |            |
 ------------------------------------------------------------------------------
 <PF1> HELP          <PF2>  RETURN   <PF3>  SHOW TABLES   <PF4>  SHOW CODES
 <PF5> COPY SECURITY <PF6>  DELETE   <PF7>  BACKWARD      <PF8>  FORWARD
 <PF9> NOT USED      <PF10> NOT USED <PF11> DELETE TABLES <PF12> DELETE CODES
```

Action

The START WITH field, located in the upper-right corner of this panel, is where you enter the full or partial name of the user where you want the listing to start. When you press ENTER, CA Dataquery refreshes the SECURITY USER DIRECTORY panel with the user that you specified on the first line of the listing. You can also page forward using <PF8> FORWARD or backward using <PF7> BACKWARD until you reach the member that you want to view and/or edit.

Panel Description

The panel provides you with a list of users who are defined in the CA Dataquery system. It does not, however tell you which users are authorized to access CA Dataquery with the external security package. The panel enables you to perform many tasks specified by the PF keys. The following list explains each column on the panel.

USER NAME

Names each user currently authorized on CA Dataquery.

DATE ADDED

Lists the date the user was added to CA Dataquery.

DATE USED

Lists the date that the user last accessed CA Dataquery.

PF Keys

The following list describes the unique PF keys for the panel-name panel.

Key	Objective	Result
<PF3> SHOW TABLES	Display tables authorized for user selected with cursor	CA Dataquery displays the Security Table List panel
<PF4> SHOW CODES	Display profile codes authorized for user selected with cursor. See How to Limit Access to Columns (see page 253)	CA Dataquery displays Security Profile Code List panel
<PF5> COPY SECURITY	Copy user authorization from user selected with cursor to another user	CA Dataquery displays Directory of User Copy Targets panel
<PF6> DELETE	Delete both table and profile code authorizations for user selected with cursor	CA Dataquery displays message indicating results
<PF11> DELETE TABLES	Delete table authorizations for user selected with cursor	CA Dataquery displays message indicating results
<PF12> DELETE CODES	Delete profile code authorizations for cursor	CA Dataquery displays message user selected with indicating results

Modifying Table Authorizations Related to One User

See Specifying Table Options Using the USER Option (see page 240) for instructions on selecting a user name on the Security User Directory panel and pressing <PF3> SHOW TABLES to see the Security Table List panel.

Security Table List (DQLG0)

```
 =>
Place the cursor on a file name to delete or update.  Use PF 3 to add tables.
-------------------------------------------------------------------------DQLG0
DATAQUERY:  SECURITY TABLE LIST        USER: _____________________________
-------------------------------------------------------------------------------
    Database ID   |   DB Table Name |  Find    Update   Insert    Erase
-------------------------------------------------------------------------------
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
                  |                 |
-------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN    <PF3>  ADD         <PF4>  UPDATE
<PF5> NOT USED      <PF6>  DELETE    <PF7>  BACKWARD    <PF8>  FORWARD
```

Panel Description

The panel lists tables currently related to the user ID you specified on the Security User Directory panel with their function authorizations. The following list explains each column on the panel.

Database ID

Lists each table name's database ID.

DB Table Name

Names each table currently secured to the user.

FIND, UPDATE, INSERT, ERASE

Represent the CA Dataquery functions which the users can be authorized to perform. A **Y** in one of these columns indicates the user can perform that particular function for the named database ID and table.

The fields on this screen are for display only. No data can be entered.

Action

To make any necessary changes or additions on the Security Table List panel, place the cursor on the line with the DB Table Name and Database ID to modify and press the appropriate PF key. <PF3> ADD, <PF4> UPDATE, and <PF6> DELETE are discussed in detail on the following pages.

PF Keys

The following list describes the PF keys:

Key	Objective	Result
CLEAR	Return to Security User List panel Menu	CA Dataquery displays the Security User List panel
<PF1> HELP	Display Help panels	CA Dataquery displays the Help panel
<PF2> RETURN	Return to previous panel	Returns to previous panel, or Main Menu
<PF3> ADD	Add new database ID and table for this user	CA Dataquery displays Security Table Maintenance panel
<PF4> UPDATE	Update a function authorization for this user	CA Dataquery displays Security Table Maintenance panel
<PF5> NOT USED	Not in use	
<PF6> DELETE	Delete a database ID and table for this user	CA Dataquery displays message indicating results
<PF7> BACKWARD	Scroll to previous page	Displays previous page
<PF8> FORWARD	Scroll to next page of list, if any	Displays the next page of list, if any

Note: To use <PF4> ADD or <PF6> DELETE, select a table/DBID using cursor position.

Changing Authorizations

To change function authorizations, select a DBID and table name with the cursor and press <PF4> UPDATE. CA Dataquery displays the following panel:

Security Table Maintenance (DQLH0)

```
=>
Enter the security information and press the appropriate PF key.
-------------------------------------------------------------------------------DQLH0
DATAQUERY:  SECURITY TABLE MAINTENANCE  USER: ____________________________________
-------------------------------------------------------------------------------
         Data Base ID           :
          DB Table Name         :          (Enter *ALL* for all tables of the
                                            database ID)

                            Find:
                          Update:
                          Insert:
                           Erase:









-------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN    <PF3>  NOT USED    <PF4>  UPDATE D
```

Note: Removing all the authorizations for a particular user deletes that user from the list the next time the user attempts to access that table and does not allow access to that table. If external security is in effect, it overrides any changes you might make on database or table authorizations.

Enter **Y** or **N** next to the functions.

If a user had access to only selected tables in a database, to authorize that user access to the entire database, enter *ALL* as the Table Name. The *ALL* authorization supersedes, but does not delete, the individual table authorizations.

For example, if a user had only FIND access to some tables and you want to give that user full access to the entire database, enter *ALL* as the Table Name and, on the next panel, add the user with FIND, UPDATE, INSERT, and ERASE authority. With the *ALL* authorization the user now has FIND, UPDATE, INSERT, and ERASE access to all tables in the database.

If the user previously had FIND and UPDATE access to a specific table and (with the *ALL* authorization) you specify FIND access to all tables in the database, the user is able to FIND any table but able to UPDATE only the specific table.

When checking authorization, CA Dataquery looks for individual specific table authorization and if that is not found, CA Dataquery looks for *ALL* authorization.

Adding Authorizations

To add a new database ID for the selected user, press <PF3> ADD. CA Dataquery displays the Security Table Maintenance panel.

Security Table Maintenance (DQLH0)

```
=>
Enter the security information and press the appropriate PF key.
-------------------------------------------------------------------------------DQLH0
DATAQUERY:  SECURITY TABLE MAINTENANCE  USER: ____________________________________
-------------------------------------------------------------------------------
         Data Base ID           :
          DB Table Name         :          (Enter *ALL* for all tables of the
                                            database ID)

                             Find:
                           Update:
                           Insert:
                            Erase:









-------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN    <PF3>  NOT USED    <PF4>  UPDATE D
```

If external security is in effect, it overrides any changes you might make on user, database, or table authorizations.

Panel Description

The panel provides the means to add authorizations to the user ID you specified on the Security Table List panel. The following list explains each column on the panel:

DATABASE ID

List the 1-3 digit database ID.

DB TABLE NAME

Names the table to be related to the user.

FIND, UPDATE, INSERT, ERASE

Represent the CA Dataquery functions which the users can be authorized to perform. A **Y** following a table name and database ID in one of these columns indicates the user can perform that particular function.

To add a table to this list of accessible tables for this user, enter the 3-digit database ID and the table name, or enter *ALL* to give the user access to all tables in this database. Press <PF3> ADD to process.

Copying Authorizations

Summary

Copying authorizations from one user to another is a quick way to authorize new users to access the same tables and columns as an existing user. If a user has similar needs as an existing user, you can modify the authorizations after completing the copy function. You can copy tables only, codes only, or both tables and codes to the new user (target).

Copying Security

Copying security is copying database tables and profile codes from one user to another. To copy security, choose the SECURITY CONTROL option from the Administration Menu. Then select USER on the Security Maintenance Menu.

The new user and the existing user have to be listed on the Security User Directory panel. For more information about creating new user IDs, see Authorizing Users in CA Dataquery.

If external security is in effect, it overrides any changes you may make on user, database, or table authorizations.

Place the cursor on the name of the user to copy and press <PF5> COPY SECURITY. CA Dataquery displays the following panel:

Directory of User Copy Targets (DQLK0)

```
=>
Place the cursor on a name for the copy target and press the PF5/17 key.
-------------------------------------------------------------------------------DQLK0
DATAQUERY:  DIRECTORY OF USER COPY TARGETS       START WITH => _________________
-------------------------------------------------------------------------------
       Using user : _____________________________  for copy source
-------------------------------------------------------------------------------
         USER NAME                | DATE ADDED | DATE USED
-------------------------------------------------------------------------------
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
                                  |            |
-------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN    <PF3>  COPY TABLES <PF4>  COPY CODES
<PF5> COPY BOTH     <PF6>  NOT USED  <PF7>  BACKWARD    <PF8>  FORWARD
```

Place the cursor on the user name who is to receive the authorizations.

Copying Tables

To copy only table authorizations to the new user, place the cursor on the new user name and select <PF3> COPY TABLES.

Copying Codes

To copy only profile code authorizations to the new user, place the cursor on the new user name and press <PF4> COPY CODES.

Copying All Authorizations

To copy all of the authorizations from one user to another, place the cursor on the new user name and select <PF5> COPY BOTH. CA Dataquery displays a message indicating that the copy was successful.

Changing the Copied Security

To change any of the copied security, return to the Security User Directory panel, use the PF keys to show codes or tables, then press the PF key to update the codes or tables. For more information, see Specifying Table Options Using the USER Option (see page 240).

Naming a CA Datacom/DB Database and Table for User Access

If external security is in effect, it overrides any changes you might make on user, database, or table authorizations. Verify that external and CA Dataquery authorizations match if you want to maintain user, database and table security with CA Dataquery and with the external package.

Action

To use CA Dataquery to specify a CA Datacom/DB database for a user to access:

Step 1

Choose the SECURITY CONTROL option from the Administrative Menu.

Step 2

Select DATABASE from the Security Maintenance Menu.

CA Dataquery displays the following panel:

Security Table Name (DQLB0)

```
 =>
Enter the appropriate information and press PF4.
-------------------------------------------------------------------DQLB0
DATAQUERY:  SECURITY TABLE NAME
-------------------------------------------------------------------------

 Enter the three-digit CA Datacom/DB Database Identifier to be used:
 Database ID :  ___

 Enter the three character CA Datacom/DB Table name:
 Table name: ___

 (Leave blank if you wish to process by
  CA Datacom/DB Database Identifier only)




 <PF1> HELP   <PF2> RETURN     <PF3> NOT USED     <PF4>  DISPLAY USERS
```

Action

Complete the panel and press <PF4> DISPLAY USERS.

Panel Description

DATABASE ID:

Enter a valid 1- to 3-digit database ID. This ID specifies the database that this user is to be authorized to access.

TABLE NAME:

Enter a valid 1- to 3-alphabetic database table name. This name is the name of the table that this user is authorized to access. Leave blank if you want to authorize the user for all tables in the specified database ID.

After you name a database and table on the Security Table Name panel, and press <PF4> DISPLAY USERS, CA Dataquery displays the Security User List panel.

Security User List (DQLC0)

```
=>
Place the cursor on a name to delete or update.  Use PF3 to add new users.
-------------------------------------------------------------------------------DQLC0
DATAQUERY:  SECURITY USER LIST                        DBID: ___ TABLE: _____
-------------------------------------------------------------------------------
          User name                |  Find  | Update | Insert |  Erase
-------------------------------------------------------------------------------
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
                                   |        |        |        |
-------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN    <PF3>  ADD         <PF4>  UPDATE
<PF5> NOT USED      <PF6>  DELETE    <PF7>  BACKWARD    <PF8>  FORWARD
```

PF Keys

The following list describes the unique PF keys on the Security User List panel.

Key	Objective	Result
<PF3> ADD	Add a user to the security list of users authorized to access this table.	Displays Security User Maintenance panel.
<PF4> UPDATE	Updates the user's authorizations.	Displays the Security User Maintenance panel.
<PF6> DELETE	Deletes a name from the Security List panel.	Removes the authorization for the user.

Note: To use <PF4> UPDATE or <PF6> DELETE, you must select a user with the cursor position.

To see the entire list, press <PF8> FORWARD until you see the message, LAST PAGE, at the bottom of the screen.

Adding a User to a Table

To add a new user, from the Security User List panel:

Step 1

Press <PF3> ADD. CA Dataquery displays the Security User Maintenance panel.

Step 2

Enter the user name and place a **Y** in the space opposite each authorized function for that user. This authorizes the functions for which you want that user to be authorized. Always authorize users for FIND in any table they are to access.

After you have added a user and authorized the functions, press <PF3> ADD. CA Dataquery verifies the user authorization.

Security User Maintenance (DQLD0)

```
=>
Enter the security information and press the appropriate PF key.
------------------------------------------------------------------------
DATAQUERY :  SECURITY USER MAINTENANCE
------------------------------------------------------------------DQLD0
          User Name           :

                        Find:
                      Update:
                      Insert:
                       Erase:









------------------------------------------------------------------------
<PF1>  HELP      <PF2>  RETURN      <PF3>  ADD      <PF4>  NOT USED
```

Using CA Datacom Datadictionary to Relate Multiple Users to Tables

When you need to add many table/user authorizations, you can use CA Datacom Datadictionary as an alternative to using the online CA Dataquery facility. Follow these steps:

Step 1

Build an entity-occurrence for the AUTHORIZATION entity-type for the performance of a function on a particular table. The format is:

```
$DQ-tttt-fffiii
```

$DQ

Constant

tttt

Identifier for the type of access or update:

- DISR for FIND (retrieval)
- UPDR for UPDATE
- ADDR for INSERT
- DELR for ERASE

fff

CA Datacom/DB table name

iii

DATABASE ID

For example, the entity-occurrence for a table named CMP in database 001 for FIND is:

$DQ-DISR-CMP001

Define your entity-occurrences to CA Datacom Datadictionary and put them in production status.

Note: For more information, see the *CA Datacom Datadictionary Online Reference Guide*.

Step 2

Add the user in online CA Dataquery. This creates an entity-occurrence within the PERSON entity-type in PROD status. For more information, see Adding a User to a Table (see page 251).

Step 3

Relate the PERSON in Step 2 to the appropriate AUTHORIZATIONS in Step 1.

Note: For more information and instructions, see the *CA Datacom Datadictionary Online Reference Guide*.

Limiting Access to Columns

CA Dataquery provides you with the ability to restrict users' access to data using profile codes, restrictions, and conditions. These security measures are maintained by CA Dataquery and are not overridden by external security.

How to Limit Access to Columns

Profile codes are used to restrict access to data in a specific column, whereas restricted conditions limit access to data in a specific row based on a particular value in the column. Effective use of profile codes allows you to prohibit unwarranted access to sensitive data at the column level.

Using Profile Codes

A PROFILE-CODE is a CA Datacom Datadictionary attribute of the FIELD entity-type used by CA Dataquery to classify fields (columns) into various security groups. Once the profile-code is established and included in the field definition, only users who are authorized for that profile-code can FIND and/or UPDATE data in the protected fields. The assignment of profile codes controls which fields the user sees on the Display Fields panel, unless the user is Data Authorized. If Data Authorized=yes on the User Authorization panel, the user can display fields but cannot update if they are protected by a profile-code.

At installation, all CA Datacom Datadictionary FIELD entity-occurrences have a null profile-code. This means that once table level authorization is granted to a user, that user has the ability to FIND every field (column) in that table. If you assign a profile-code to a column however, only those users authorized for that profile-code can FIND and/or UPDATE that column.

For example, say you have columns occurring on several rows that contain financial information. Perhaps one column contains prices of inventory items, another contains information on discount rates for certain customers. If you do not want all of your users to have access to this information, you assign a profile-code to each column, or you use one profile-code for both. For this example, use the code MONY for both columns. Then decide which users can access MONY columns.

If a simple column is named in a query and does not have a profile-code assigned, it is secured by the profile-code of its parent or grandparent, if one exists. If these columns do not have profile codes, the simple columns stated in the query are unprotected and available to any user with table level authorization.

If a compound field is named in a query and does not have a profile-code assigned, it receives a profile-code belonging to its parents or grandparents if one exists. If its parents or grandparents do not have a profile-code, the code of its children or grandchildren is in effect. If none of these fields has a profile-code, the field is unprotected and available to any user with table level authorization. If a compound field has a profile-code assigned, be aware that all columns that make up the compound column have the same profile-code.

Note: TheCA Datacom Datadictionary REDEFINES attribute, which is not recognized by CA Dataquery, needs to be handled separately. For example, if FIELD X is assigned a profile-code ABC, and FIELD Y redefines X, the profile-code ABC does not carry over to FIELD Y. You need to assign the profile-code ABC to FIELD Y.

If you are planning your CA Dataquery security needs prior to creation of your database, contact the Database Administrator regarding your field security needs, so that profile codes can be established and included in the field definitions. Establish the users' authorizations to profile codes using the CA Dataquery SECURITY CONTROL administrative function.

The CA Dataquery SECURITY CONTROL function provides the following options:

SHOW CODES

This option allows you to assign CA Datacom Datadictionary profile codes which protect sensitive column data to users who need access to the protected data. A profile-code is an attribute of a column used by CA Dataquery to classify columns into various security groups. Once a profile-code is established and included in the column definition, only users who are authorized for that code can access data in the protected columns. If **Y** (yes) has been specified on the DATA AUTHORIZED field on the User Table Maintenance panel, a user without profile-code authorization can read the data.

COPY SECURITY

This option allows you to copy to another user one or all of the authorizations that have been assigned to one user. The security access can remain the same or be further modified for the new user.

COPY CODES

This option allows you to copy the profile codes assigned to one user to another user. Another method of restricting access to data is the use of conditions and restrictions. Conditions are created which qualify access to rows of data based on data values. for more information, see Limiting Access to Rows Using Conditions and Restrictions (see page 257).

Authorizing Access to Protected Columns

Relating a user to a profile-code allows that user to access columns protected by CA Datacom Datadictionary profile codes. Plan carefully before using this function. See your Security Administrator to gain a complete understanding of the implications of profile-code relationships to be sure that you are following the Security Administrator's security plan.

To establish, display, modify, or delete profile-code relationships for one user, choose the SECURITY CONTROL option from the Administrative Menu. Then select USER on the Security Maintenance Menu. CA Dataquery displays the Security User Directory panel. To go directly to the Security User Directory panel, enter SECURITY USER on the command line.

Viewing and Modifying Profile Codes Related to One User

Place the cursor on the user name on the Security User Directory panel. Press <PF4> SHOW CODES, to see the Security Profile Code List panel.

Security Profile Code List (DQLI0)

```
-------------------------------------------------------------------DQLI0
DATAQUERY:  SECURITY PROFILE CODE LIST   USER:
-------------------------------------------------------------------------
   PROFILE CODE  |  FIND  |  UPDATE
-------------------------------------------------------------------------
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
                 |        |
 LAST PAGE-------------------------------------------------------------
 <PF1>  HELP      <PF2>  RETURN  <PF3>  ADD       <PF4>  UPDATE
 <PF5>  NOT USED  <PF6>  DELETE  <PF7>  BACKWARD  <PF8>  FORWARD
```

Listed under the PROFILE CODE column heading are the profile codes currently related to the user. A **Y** in the columns, FIND and UPDATE, indicates that the user can perform those functions. You can add, modify or delete profile codes and function authorizations on this screen using the PF keys.

Deleting

To delete a profile-code authorization, place the cursor on the profile-code on the Security Profile Code List panel (DQLI0) and press <PF6> DELETE.

Changing

To add or delete a function authorization to an existing authorized profile-code, place the cursor on the profile-code and press <PF4> UPDATE. Place a **Y** opposite the function to be added. To remove authorization for a function, tab to the appropriate field and enter an **N**. Removing all the authorizations for a particular profile-code deletes that code from the list the next time the function is selected.

Adding Profile-Code Authorizations

To assign a user authorization to a profile-code and/or its functions, press <PF3> ADD. CA Dataquery displays the following panel:

Security Code Maintenance (DQLJ0)

```
 =>
 Enter the security information and press the appropriate PF key.
--------------------------------------------------------------------------------DQLJ0
 DATAQUERY:  SECURITY CODE MAINTENANCE  USER: ____________________________ ______
--------------------------------------------------------------------------------
           PROFILE CODE          :

                             FIND:
                           UPDATE:









 --------------------------------------------------------------------------------
 <PF1> HELP           <PF2>  RETURN         <PF3>  ADD          <PF4>  NOT USED
```

Enter the name of the profile-code and place a **Y** opposite the function to be assigned to this user. Press the <PF3> ADD key to process this assignment. CA Dataquery displays a message indicating that the add is successful.

Limiting Access to Rows Using Conditions and Restrictions

CA Dataquery provides you with the ability to restrict users' access to data using profile codes, restrictions, and conditions. These security measures are maintained by CA Dataquery and are not overridden by external security.

As the CA Dataquery Administrator, you can restrict access to data in a named database according to the value of the data itself. The vehicle which names the values that cannot be retrieved is called a *restriction.*

You assign a restriction to an individual user or a user group. A restriction consists of one or more *conditions* that prevent retrieval of specific data. A typical condition is *ZIP CODE NOT EQUAL 75044*. When a query (or dialog) executes against the restricted database, CA Dataquery inserts the conditions in the query and thus qualifies the data that is retrieved. With this method, you apply additional qualifications to a user's queries, allowing the user to view only those rows which satisfy both the query and the user's assigned restricted condition(s).

To restrict a user, follow these steps:

Step 1

Define the condition, giving it a name.

Step 2

List its name on the panel that defines a named restriction.

Step 3

Decide which user or group of users to restrict with the condition. Use the RESTRICTIONS option on the Administrative Menu to assign the condition to an individual user.

Maintaining Conditions

A condition is appended with an AND to any query or dialog in which the user accesses a table for which data access is restricted. For example,

```
FIND ALL SALES WITH YTD-SALES GT 1000
 AND id=15 AND CITY=DALLAS
```

This condition limits the users access to data based on the content of the data in two columns. id=15 allows the user to access only those rows in the table in which the value of the ID is equal to 15. Any other rows where the ID is not equal to 15 are not accessible. Furthermore, this condition limits access to those rows in which ID=15 *and* CITY=DALLAS. If a row met the first condition criteria, id=15, but did not meet the second condition criteria, CITY=DALLAS, the user would be unable to access any data in that row. The only data the user can access is in the rows that meet the criteria specified in the condition.

Access Conditions

To create, view, or edit a condition, begin by selecting the CONDITIONS option from the Administrative Menu, or use the CONDITION command from the command line. CA Dataquery displays the Directory of Conditions. A sample Directory of Conditions panel follows:

Directory of Conditions (DQKW0)

```
=>
Place the cursor on a name to delete or edit and press the appropriate PFkey
-------------------------------------------------------------------------------DQKW0
DATAQUERY: DIRECTORY OF CONDITIONS               START WITH: _______________
-------------------------------------------------------------------------------
     CONDITION NAME                |  TABLE NAME
-------------------------------------------------------------------------------
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
-------------------------------------------------------------------------------
<PF1>  HELP       <PF2>  RETURN       <PF3>  CREATE       <PF4>  EDIT
<PF5>  NOT USED   <PF6>  DELETE       <PF7>  BACKWARD     <PF8>  FORWARD
```

Action

The START WITH: field, located in the upper-right corner of this panel, is where you enter the full or partial condition where you want the listing to start. When you press Enter, CA Dataquery displays the condition specified on the first line of the listing. You can also page forward using <PF8> FORWARD or backward using <PF7> BACKWARD until you reach the member that you want to view and/or edit.

Panel Description

The following list describes each column of the Directory of Conditions panel.

CONDITION NAME

Alphabetical listing of all existing conditions.

TABLE NAME

Name of the table to which this condition applies.

PF Keys

The following PF keys are unique to the Directory of Conditions panel. The remainder of this section explains each function.

Key	Objective	Result
<PF3> CREATE	Create a new condition	CA Dataquery displays the Editor panel
<PF4> EDIT	Display or modify an existing condition	Display that condition on the Editor panel
<PF6> DELETE	Delete a condition	CA Dataquery removes that condition

Note: <PF4> EDIT and <PF6> DELETE require selection of a condition using the cursor position.

Creating a Condition

When you want to create a new condition, choose the CONDITIONS option from the Administrative Menu, or use the CONDITION command on the command line. When the Directory of Conditions panel appears, press <PF3> CREATE to create a new condition. CA Dataquery then displays the Editor panel allowing you to input your condition. An explanation of the Editor panel appears in the *CA Dataquery User Guide*.

Following is a sample Editor panel that appears when you press <PF3> CREATE during display of the Directory of Conditions.

Sample Editor Panel from the Dir. of Conditions

```
=>
CREATION PANEL
--------------------------------------------------------------------------------DQD10
DATAQUERY:  EDITOR           CURRENT TABLE:  _____________________________
--------------------------------------------------------------------------------
NAME:          _______________                  TYPE: COND__
DESCRIPTION:   ____________________________________________________________
   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+.
.. ================================ T O P ===================================
..
..
..
..
..
..
..
..
..
.. ============================ B O T T O M ===================================

--------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN     <PF3>  NOT USED       <PF4>  SAVE
<PF5> NOT USED      <PF6>  DELETE     <PF7>  BACKWARD       <PF8>  FORWARD
<PF9> UPDATE        <PF10> NOT USED   <PF11> RIGHT/LEFT     <PF12> NOT USED
```

Action

Complete the top of the panel and write the condition in the text area of the panel.

NAME

Enter the 1- to 15-character alphanumeric name for this condition. Supply the table name on which this condition is based in the Current Table field. Remember to give your condition a unique name.

TYPE

CA Dataquery supplies COND to specify that this is a condition and is to be saved in the condition library.

DESCRIPTION

Enter explanatory information about this condition. CA Dataquery displays this description on the Directory of Conditions panel and other condition-related panels.

When the top of the panel is complete, enter the condition. Conditions can either include WITH or not. Either way is valid. Follow the rules for WITH clauses as described in the *CA Dataquery Reference Guide*. Press <PF4> SAVE to save the condition.

Next Step

The next step in applying the condition to a specific table is to assign the condition to a restriction definition. Select RESTRICTIONS from the Administrative Menu and see Using Conditions to Restrict Data (see page 262).

Examples

Some examples of conditions are:

```
ZIPCODE='75243'

CITY NE 'DALLAS'
```

Modifying Existing Conditions

To modify an existing condition, select the CONDITIONS option from the Administrative Menu, or use the CONDITION command from the command line. When CA Dataquery displays the Directory of Conditions panel, scroll through the listing of condition names until you display the condition you want to edit. Position the cursor beside that condition and press <PF4> EDIT. CA Dataquery displays that condition on the Editor panel.

When you have finished making changes to the condition, press <PF9> UPDATE to update the condition library with this new version. If you leave the Editor panel without pressing <PF9> UPDATE, CA Dataquery does not replace the original version of the condition with the displayed modified version. If you want to retain your original version and also save your modified version, type a new name over the original name and press <PF4> SAVE to save the new version.

Deleting Conditions

To delete a condition from CA Dataquery, select the CONDITIONS option from the Administrative Menu, or use the CONDITION command from the command line. When CA Dataquery displays the Directory of Conditions panel, scroll through the listing of condition names until you display the condition you want to delete. Position the cursor beside that condition and press <PF6> DELETE. CA Dataquery immediately deletes that condition and refreshes the panel. All restrictions containing the deleted condition should be updated, although, the deleted condition is ignored when the restriction is applied at query execution.

Once you have deleted a condition from the Directory of Conditions panel, that condition no longer exists. If you have made an error, you must re-create that condition or restore it from a backup.

You can also delete a condition while viewing it on the Editor panel. Because the condition displayed on the Editor panel is in the Active Query Area, the deleted condition can be immediately restored by entering EDIT * in the command field. When CA Dataquery redisplays the condition, you must save that condition as if it were a new condition by pressing <PF4> SAVE.

Using Conditions to Restrict Data

Summary

A restriction is a list of 1 to 40 conditions which are to be applied to the specified user or group when they access a given table.

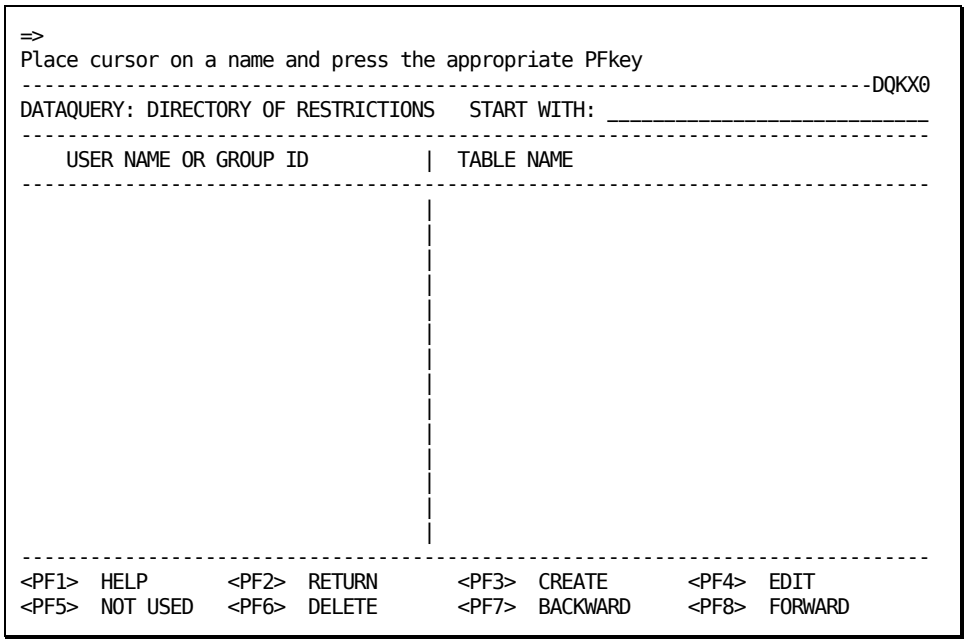
Another method of restricting access to data is the use of profile codes. Profile codes are applied through CA Datacom Datadictionary to specific columns in a table so that only users who are related to the profile codes can access the data in a restricted column. (Data authorized users have read-only access even on columns protected by profile codes.) Conditions prevent access to a whole row based on data values.

The user and/or group(s) can access only the rows (based on the content of the data in the row) in the specified table that do not contain restricted data. The table specified in the restriction must match the table specified in each listed condition. For more information about conditions, see Maintaining Conditions (see page 258). There can be only one restriction per user per table and one restriction per group per table. If an individual user is assigned both an individual and a group restriction, both are applied.

Action

Once you know which table-related conditions you want to apply to a user or group to limit their access to a particular table, select RESTRICTIONS from the Administrative Menu, or use the RESTRICT command from the command line. CA Dataquery responds by displaying the Directory of Restrictions panel. A sample Directory of Restrictions panel follows:

Directory of Restrictions (DQKX0)



Action

The START WITH: field, located in the upper-right corner of this panel, is where you enter the full or partial name of the user name or group ID where you want the listing to start. When you press Enter, CA Dataquery refreshes the Directory of Restrictions panel with the user or group ID that you specified on the first line of the listing. You can also page forward using <PF8> FORWARD or backward using <PF7> BACKWARD until you reach the member that you want to view and/or edit.

Panel Description

The following list describes each column of the Directory of Restrictions panel.

USER NAME or GROUP ID

Alphabetical listing of all existing users and groups for which there is a restricted condition.

TABLE NAME

Table for which this condition has been created.

PF Keys

The following list describes the PF keys on the Directory of Restrictions panel.

Key	Objective	Result
<PF3> CREATE	Create a new restriction	CA Dataquery displays the Editor panel
<PF4> EDIT	Modify an existing restriction	Displays that restriction
<PF6> DELETE	Delete a restriction	CA Dataquery removes that restriction

Note: <PF4> EDIT and <PF6> DELETE require selecting a restriction using the cursor position.

Using Restricted Conditions

When you need to allow users access to some, but not all, of the rows in a table, you use restricted conditions. When you restrict access by column content (the value at the intersection of every row and column) you restrict access to part of the data within that table. You define the condition, giving it a name, identifying the table, and stating the condition. For instance, the condition may restrict access to all SALES rows containing a value of 15 in the column for sales ID and a value of DALLAS in the city column. The administrator who is authorized to access the CONDITIONS function creates the condition following your specifications.

A condition results in restricting the user's access to data in that table. That user can only access data that meets the qualifications of the condition. In the condition shown next, the user is permitted to access only those rows that have an ID of 20 and a city of Dallas.

```
WITH id=20 AND CITY=DALLAS
```

CA Dataquery automatically appends the condition to the DQL Language query or DQL Language dialog. The condition is transparent to the user.

You also decide which user or group of users to restrict with the condition. The administrator with RESTRICTIONS authorization assigns the condition(s) to an individual user. If you have assigned group levels to users that identify them as belonging to specific groups, you can restrict the condition(s) to a group(s).

For example, if you have defined a high-order (level 1) group named Sales, a middle-order (level 2) group named Dallas, and a low-order (level 3) group named Clerical, and if your company maintains sales rows for all branches in the same table and each row contains a branch code. The branch codes may be:

- Austin - 10
- Dallas - 20
- Houston - 30
- Midland - 40

If you want clerical users in the Dallas branch to access only the rows for their branch, you create a restricted condition that prevents them from accessing rows that do not contain a 20 in the column for branch codes. Then you assign that restricted condition to all users having a high-order level 1 group of Sales, middle-order level 2 group of Dallas, and a low-order level 3 group of Clerical. You could, of course, assign the restriction to each user individually, if you prefer. Assigning by groups simplifies administration when personnel change job functions or move within the organization of your company frequently.

A restriction can contain multiple conditions. The maximum is 40 conditions and the minimum is 1 condition. The condition must apply to the same CA Datacom/DB table as the restriction. The restriction is then assigned to a user and/or a group level(s).

You cannot restrict access to data using Conditions and Restrictions in SQL Mode.

Creating or Modifying a Restriction

To create or modify an existing restriction, choose the RESTRICTIONS option from the Administrative Menu, or use the RESTRICT command from the command line. When the Directory of Restrictions panel appears, position the cursor next to a restriction and press <PF3> EDIT to modify an existing restriction. CA Dataquery then displays the Restriction Edit panel, as shown in the following example, allowing you to modify the existing restriction relative to a user or group.

Restriction Edit (DQKA0)

```
=>
OVERTYPE THE CONDITIONS TO BE MODIFIED AND PRESS <PF4> TO COMPLETE THE UPDATE
-------------------------------------------------------------------------------DQKA0
DATAQUERY:  RESTRICTION EDIT
--------------------------------------------------------------------------------
USER          ____________________________
GROUP ID: LV1 _______________  LV2 _______________  LV3 _______________
TABLE:        ____________________________
--------------------------------------------------------------------------------
CONDITIONS:
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
--------------------------------------------------------------------------------
<PF1>  HELP       <PF2>  RETURN   <PF3> DISPLAY CONDITION <PF4>  SAVE
<PF5>  LIST CONDS <PF6>  DELETE   <PF7> NOT USED          <PF8>  NOT USED
```

Panel Description

A list of the fields and descriptions from the Restriction Edit panels follows.

USER

Enter the user name to whom this restriction applies. If you do not enter a user name, you must specify a Group ID.

GROUP ID:

Specify one of the following against which this restriction is to apply.

- A group level 1 (LV1)
- A group level 1 (LV1) and a group level 2 (LV2),
- A group level 1 (LV1) and a group level 2 (LV2), and a group level 3 (LV3) group ID

If you do not enter a group ID, you must enter a user name.

TABLE:

Enter the CA Datacom Datadictionary TABLE entity-name that names the table to which you want to limit access. CA Dataquery requires that the condition applies to the same table as the associated restriction.

CONDITIONS:

Enter one or more condition names which are to restrict the user's and group's access to the named table. The conditions named are connected by AND and processed at query execution time.

Displaying a Condition

To review a condition that you have listed on the Restriction Edit panel, press <PF3> DISPLAY CONDITION. (The cursor must be positioned by the condition name.) CA Dataquery displays that condition on the Editor panel. Press <PF2> RETURN when you have finished viewing the condition to return to the Restriction Edit panel.

Saving Your Restriction

When you are creating or editing a restriction on the Restriction Edit panel, you must save your work. Simply press <PF4> SAVE before leaving this panel. CA Dataquery saves your new restriction, lists it on the Directory of Restrictions panel, and puts it into effect for the designated user(s) and/or group(s) when they execute a query that accesses the table to which this restriction applies. (If you have applied a condition to a user who is outside of your group, the assignment will not be listed on your panel, even though it exists.)

Viewing a Listing of Existing Conditions

When you are viewing the Restriction Edit panel, you might want to refresh your memory as to what the names of the existing conditions are and their associated table names. When you press <PF5> LIST CONDS, CA Dataquery displays the Directory of Conditions panel for that purpose. For more information about the Directory of Conditions panel, see Maintaining Conditions (see page 258).

Deleting a Condition Within a Restriction

When you want to remove one or more conditions imposed on a user and/or a group, begin by selecting the RESTRICTIONS option from the Administrative Menu, or use the RESTRICT command from the command line. When CA Dataquery displays the Directory of Restrictions panel, position the cursor beside the user name or group ID that you want to modify. Then press <PF4> EDIT to display the Restriction Edit panel.

Position the cursor on the condition name that you want to delete and blank it out, or use Erase End of Field and press <PF4> SAVE to save. CA Dataquery immediately deletes that condition and refreshes the panel. The change in the restriction is not applicable to any user or group ID listed in the restriction until the next time that a query is executed that accesses that restricted table.

CA Dataquery requires that a restriction must contain at least one condition.

Deleting a Restriction

When you need to remove a restriction from a user or group, begin by selecting the RESTRICTIONS option from the Administrative Menu, or using the RESTRICTIONS command from the command line. CA Dataquery displays the Directory of Restrictions panel, as shown in the following example:

Directory of Restrictions (DQKX0)

```
=>
Place cursor on a name and press the appropriate PFkey
-------------------------------------------------------------------------------DQKX0
DATAQUERY: DIRECTORY OF RESTRICTIONS   START WITH: _____________________________
-------------------------------------------------------------------------------
    USER NAME OR GROUP ID          |  TABLE NAME
-------------------------------------------------------------------------------
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
                                   |
-------------------------------------------------------------------------------
<PF1>  HELP       <PF2>  RETURN       <PF3>  CREATE       <PF4>  EDIT
<PF5>  NOT USED   <PF6>  DELETE       <PF7>  BACKWARD     <PF8>  FORWARD
```

Action

Scroll through this panel until you locate the user or group name and its associated table name. Position the cursor beside the user or group and press <PF6> DELETE. CA Dataquery immediately deletes that restriction and refreshes the panel. The restriction is no longer in effect when the user or a user assigned to the group accesses the previously restricted table.

For an explanation of the fields and PF keys for the Directory of Restrictions panel, see Using Conditions to Restrict Data (see page 262).

Sample Condition and Restriction

The following is a step-by-step example of how to create a restricted condition using the Sample Order Entry Database.

Assume that your company has sales offices in New York, San Francisco, Dallas, and Atlanta. In each sales office is an accounting department. The accounting department in Dallas does not need to access data for any state except Texas from the CA-CUST-REC table. To restrict the CPAs in the Dallas sales office to records from the CA-CUST-REC table with STATE=TX, perform the following steps:

Step 1

Assign these group levels to all CPAs in Dallas using the USERS option on the Administrative Menu:

- Group Level 1 = SALES
- Group Level 2 = DALLAS
- Group Level 3 = ACCOUNTING

Sample User File (Table) Maintenance (DQKN0)

```
=>
Enter the user information and press the appropriate PF key
--------------------------------------------------------------------------------DQKN0
DATAQUERY:  USER FILE MAINTENANCE
--------------------------------------------------------------------------------
 USER NAME           : DALCPA1
 PASSWORD            :                          OPTIONAL
 ACCOUNTING CODE     :                          OPTIONAL
 QUERY LANGUAGE      :  DQL                     SQL OR DQL
 SQL AUTHORIZATION ID:                          REQUIRED FOR SQL OR PDB
 GROUP LEVEL 1       :  SALES                   OPTIONAL
 GROUP LEVEL 2       :  DALLAS                  IF USED, LEVEL 1 REQUIRED
 GROUP LEVEL 3       :  ACCOUNTING              IF USED, LEVEL 2 REQUIRED
DQ SYSTEM STATUS.
 DATA AUTHORIZED     :    ASSOCIATE USER       :    PERSONAL DATABASE      :
 SUBMIT ALLOWED      :    EXPORT ALLOWED       :    EMAIL ALLOWED          :
 SQL AND DQL ALLOWED :    SQL DATA DEF ALLOWED :    SQL DATA MAINT ALLOWED :
SYSTEM ADMINISTRATIVE MENU ITEMS AUTHORIZED FOR.
 CONDITIONS          :    RESTRICTIONS         :    PRINTER CONTROL        :
 JCL MAINTENANCE     :    DIAGNOSTICS          :    LANGUAGE               :
 USER MAINTENANCE    :    FOUND SET MAINT      :    QUERY LIBRARY MAINT    :
 SECURITY            :
--------------------------------------------------------------------------------
<PF1> HELP      <PF2> RETURN       <PF3> ADD          <PF4> OVERRIDE DEFAULTS
```

Step 2

Create a condition using the CONDITIONS option on the Administrative Menu for the CA-CUST-REC table which states:

```
WITH STATE = 'TX'
```

Sample Condition

```
=>
CREATION PANEL
--------------------------------------------------------------------------------DQD10
DATAQUERY:  EDITOR           CURRENT TABLE:  CA-CUST-REC___________________
--------------------------------------------------------------------------------
NAME:          CPA-COND_______                    TYPE: COND__                _
DESCRIPTION:   ____________________________________________________________
   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+.
.. ============================== T O P ===================================
.. WITH STATE = 'TX'
..
..
..
..
..
..
..
..
..
   =========================  B O T T O M  ================================
--------------------------------------------------------------------------------
<PF1> HELP          <PF2>  RETURN     <PF3>  DISPLAY FIELDS <PF4>  DISPLAY KEYS
<PF5> DISPLAY ALL   <PF6>  LIST TABLES<PF7>  BACKWARD       <PF8>  FORWARD
<PF9> TEMPLATE      <PF10> VALIDATE   <PF11> RIGHT/LEFT     <PF12> PROCESS MODE
```

Step 3

Create a restriction for the CA-CUST-REC table specifying the groups as SALES, DALLAS, and ACCOUNTING and listing the condition created in Step 2 named CPA-COND. Press <PF4> SAVE to save the restriction.

Sample Restriction

```
=>
OVERTYPE THE CONDITIONS TO BE MODIFIED AND PRESS <PF4> TO COMPLETE THE UPDATE
-------------------------------------------------------------------------------DQKA0
DATAQUERY:  RESTRICTION EDIT
-------------------------------------------------------------------------------
OPERATOR      _____________________________
GROUP ID: LV1 SALES_____________  LV2 DALLAS_________  LV3 ACCOUNTING_____
TABLE:        CA-CUST-REC_____________________
-------------------------------------------------------------------------------
CONDITIONS:
    CPA-COND_______  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
    _______________  _______________  _______________  _______________
-------------------------------------------------------------------------------
<PF1>  HELP       <PF2>  RETURN   <PF3> DISPLAY CONDITION <PF4>  SAVE
<PF5>  LIST CONDS <PF6>  DELETE   <PF7> NOT USED          <PF8>  NOT USED
```

You have now successfully restricted access to data in the CA-CUST-REC table. Users whose group assignments match these are restricted using the CPA-COND condition when they try to access the CA-CUST-REC table. An additional selection criteria, WITH STATE = 'TX' has been added to any qualifying criteria which the user presents to access this table.

Condition/Restriction Reporting (DQCRRPT)

If you have condition/restriction authorization specified on the Administrative Menu you can request Condition/Restriction reports using the DQCRRPT utility. A Status Report is printed at the end of the report that indicates if the request was successful or if an error was found in the request.

- Condition reports print the following for each condition:
  - The name of the condition
  - The table name
  - The text of the condition
  - A list of the restrictions in which the condition appears
- Restriction reports print the following for each restriction:
  - The name of the restriction
  - The user or group to which the restriction applies
  - A list of all conditions within the restriction
  - The text of each condition

Action

Use the report control statements to identify the functions performed by DQCRRPT. A maximum of 60 report and maintenance control statements is allowed. There are five types of report control statements:

SIGN/ON

(Required) Specifies the user ID and password. Only one SIGN/ON statement is allowed and it must be the first statement in the job stream.

REPORT

(Required) Specifies the title of the report to be produced with this run, and the Restrictions and the Table name to be reported.

CONDITION

(Optional) Specifies the Condition name for the report to be produced with this run.

USER

(Optional) Specifies the userid for the report to be produced.

GROUP

(Optional) Selects the group for the report to be produced.

Enter the control statements in the following sequence:

For Condition Reports:

- SIGN/ON
- REPORT
- CONDITION

For Restriction Reports:

- SIGN/ON
- REPORT
- USER
- GROUP

SIGN/ON Statement

For all of the functions, the first control statement is the SIGN/ON statement. The SIGN/ON control statement is formatted as follows:

SIGN/ON

Specifies the user ID and password. Only one SIGN/ON statement is allowed and it must be the first statement in the job stream.

userid

Specifies the user ID of the person executing the DQCRRPT utility.

Valid Entries:

A 1- to 32-character user ID

Default Value:

(No default)

password

Specifies the password of the person executing the DQCRRPT utility. The password is only required when one has been assigned to the user ID.

Valid Entries:

A 1- to 9-character password

Default Value:

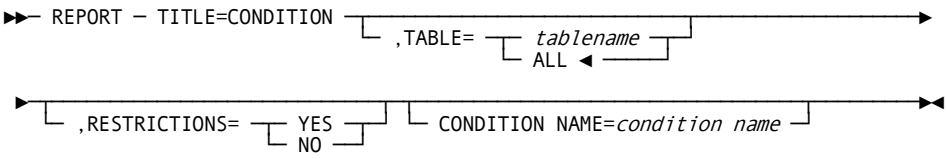
(No default)

The control statement SIGN/ON is formatted as follows:

1-8

Identifies the type of control statement. The valid entry is SIGN/ON. Left justify the value with one trailing blank, followed by the user ID.

Condition Reports



REPORT Statement

The condition REPORT statement follows the SIGNON statement in the job stream. The control statement REPORT is formatted as follows:

1-10

Identifies the type of control statement. The only valid entry is REPORT. Left justify the value with trailing blanks as necessary.

11-72

Specifies the option keywords and their values:

TITLE=

Specifies the type of report to be executed.

Valid Entries: CONDITION

Default Value: (No default)

,TABLE=

Specifies the name of the table for which conditions are to be reported (or ALL to report conditions for all tables).

Valid Entries: A 1- to 32-character table name or ALL

Default Value: ALL

,RESTRICTIONS=

Specifies whether you want to have the restrictions reported for each condition.

Valid Entries: YES or NO

Default Value: NO

There are no spaces in the keyword portion of the statement. An equal sign (=) separates an option type from its value and a comma separates the options. Do not enter options past column 72. Left justify the value with trailing blanks as necessary.

CONDITION Statement

If specified, the CONDITION statement follows the REPORT statement in the job stream. Unless a CONDITION statement is coded, all conditions are reported. Any table named on REPORT statement applies to the CONDITION statements that follow. The CONDITION statement is formatted as follows:

1-10

Identifies the type of control statement. The only valid entry is CONDITION. Left justify the value with trailing blanks as necessary.

11-72

Specifies the optional keywords and values. The NAME= keyword is required if a condition statement is coded.

NAME=

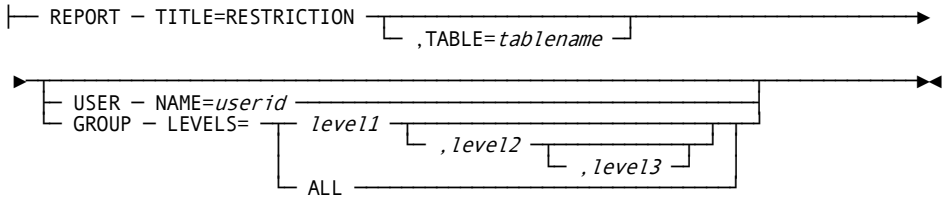
Specifies the name of the condition to be reported.

Valid Entries: A 1- to 15-character condition name

Default Value: (No default)

Note: You can request multiple reports that list single conditions by using the NAME= statement.

Restriction Reports



REPORT Statement

The Restriction REPORT statement follows the SIGNON statement in the job stream. The control statement REPORT is formatted as follows:

1-10

Identifies the type of control statement. The valid entry is REPORT.

11-72

Specifies the option keywords and their values. All Conditions within a Restriction are listed on a Restriction Report. The valid entries are:

TITLE=

(Required) Specifies the type of report to be executed.

Valid Entries: RESTRICTION

Default Value: (No default)

,TABLE=

(Optional) Specifies the name of the table to be reported.

Valid Entries: A 1- to 9-character table name

Default Value: All tables are reported.

Any table named on REPORT statement applies to USER and GROUP statements that follow. The default is ALL.

There are no spaces in the keyword portion of the statement. An equal sign (=) separates an option type from its value, and a comma separates the options. Do not enter options past column 72.

USER and GROUP Statements

The optional USER or GROUP statement is formatted as follows:

1-10

Identifies the type of control statement. Valid entries are USER and GROUP.

11-72

Specifies the option keywords and their values, as described next:

NAME=

Identifies the userid to be reported. NAME= is required if a USER statement is coded.

Valid Entries: A CA Dataquery userid

Default Value: All users are reported

LEVELS=

Specifies one to three group names to be reported. LEVELS= is required if a GROUP statement is coded. To report on all groups, code LEVELS=ALL or omit the GROUP statement.

Valid Entries: A CA Dataquery userid

Default Value: All users are reported

There are no spaces in the keyword portion of the statement. An equal sign (=) separates an option type from its value, and a comma separates the options. Do not enter options past column 72. If no USER or GROUP statements are coded, CA Dataquery reports all restrictions. You can use multiple USER and GROUP statements following the REPORT statement.

DQCRRPT JCL Samples

The following is a sample DQCRRPT JCL.

Note: Use the following as a guide to prepare your JCL. The JCL statements are for example only. Lowercase letters in a statement indicate a value you must supply. Code all statements to your site and installation standards.

Sample z/OS JCL

```
//jobname    See the note above and Listing Libraries for CA Datacom Products.
//       EXEC PGM=DQCRRPT
//STEPLIB    See the note above and Listing Libraries for CA Datacom Products.
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*                          Print Output
//SNAPER   DD SYSOUT=*
//SYSIN    DD *                                 Command input
SIGN/ON userid PASSWORD password
REPORT    TITLE=CONDITION,TABLE=PAYROLL
CONDITION NAME=TAXES
REPORT    TITLE=CONDITION
REPORT    TITLE=RESTRICTION,TABLE=PAYROLL
GROUP     LEVELS=LEVEL1,LEVEL2,LEVEL3
GROUP     LEVELS=LEVEL1
USER      NAME=userid
REPORT    TITLE=RESTRICTION
/*
//
```

Sample z/VSE JCL

```
 * $$ JOB ...       See the note above and Listing Libraries for CA Datacom Products.
 * $$ LST ...
 // JOB name
 // EXEC PROC=procname  Whether you use PROCs or LIBDEFs, see Listing Libraries for
CA Datacom Products.
 // EXEC DQCRRPT
 SIGN/ON userid PASSWORD password
 REPORT    TITLE=CONDITION,TABLE=PAYROLL
 CONDITION NAME=TAXES
 REPORT    TITLE=CONDITION
 REPORT    TITLE=RESTRICTION,TABLE=PAYROLL
 GROUP     LEVELS=LEVEL1,LEVEL2,LEVEL3
 GROUP     LEVELS=LEVEL1
 USER      NAME=userid
 REPORT    TITLE=RESTRICTION
 /*
 /&
 * $$ EOJ
```

Securing Data Access for SQL Use

Security is an important consideration in the use of SQL.

When you authorize users to use SQL, *only* CA Datacom/DB data security is in effect which means that CA Dataquery assumes that the user can access the entire database. Consult with the CA Datacom/DB Security Administrator for a complete understanding of CA Datacom/DB security.

CA Dataquery Security provides the following security measures for SQL Mode:

- Password access on a system, query group, or individual level
- SQL Mode authorization to use
  - SQL
  - Specific SQL commands

    INSERT, UPDATE, and DELETE

    CREATE, COMMENT ON, DROP, GRANT, and REVOKE
  - Personal tables
- Query access

Assigning Password Access

CA Dataquery provides the ability to assign passwords on:

- An individual level allowing each user to access CA Dataquery who has an authorized password
- Query group level allowing authorized users to access CA Dataquery if they have the authorized group password
- A system level allowing all users to access CA Dataquery who use the assigned system password

Limiting SQL Authorization

CA Dataquery provides your users with access to SQL with the option of using:

- SELECT only
- Data Definition Language with use of CREATE, COMMENT ON, DROP, GRANT, and REVOKE commands
- Data Maintenance Language with use of INSERT, UPDATE, and DELETE commands

We suggest that you limit authorization to Data Definition Language and Data Maintenance Language to a CA Dataquery Administrator. The CA Dataquery Administrator can create the necessary queries to perform these functions on the tables and/or data where appropriate, thus safeguarding the integrity of your system and its data.

Limiting Access to Queries

When the DQOPTLST parameter, QRYGRPS=YES, is specified, you can assign group IDs to a query allowing only the users assigned to those group IDs access to that query. When QRYGRPS=YES, only the administrator authorized to the LIBRARY function can update or delete that query. If QRYGRPS=NO, the author of a public or private query and the CA Dataquery Administrator can update or delete the query.

The mode (DQL or SQL) and the authorization control access to a query. DQL Mode users can access a DQL Language query, but cannot access SQL queries unless they are authorized to use SQL and are using SQL Mode at the time. SQL users can access only SQL queries unless authorized to use DQL Mode as well.

If the query is private, only the author of the query and the authorized administrator are permitted to access the query regardless of the value assigned to the QRYGRPS= parameter. If QRYGRPS=YES, and the query is public and not assigned to a group, all users can access the query. If a query's group assignments are all blank, all users can access that query. All of the user's accessible queries are displayed on that user's query library listing.

Since queries access the information in the database as defined in the query itself, the definition of the query as public or private and the assignment of the query to a group or multiple groups impacts the integrity of your data security. A user can only access those queries that they have created (if they are a conventional user), those that are public, and, if QRYGRPS=YES, those that are assigned to the group IDs matching the user's group IDs and the matching mode.

The DQOPTLST macro parameter, QRYGRPS=, has to be specified as YES so that you can implement the group assignments to queries. If QRYGRPS=NO, CA Dataquery ignores group level IDs in determining access to a query.

Using Schemas

When a user is added with a private SQL authorization specified, such as is required for SQL use, CA Dataquery automatically creates a schema in CA Datacom Datadictionary for the SQL authorization ID. A schema defines the individual user's SQL environment. Users must have a schema associated with an authorization ID to use SQL. A schema contains all table, view and privilege definitions owned by a given authorization ID. Any definitions created by the user are automatically added to the schema for the authorization ID specified when he creates the SQL object.

AUTHIDs or schemas are not used for security. SQL security (CA Datacom/DB security) is based on accessor ID and not an AUTHID.

Creating Personal Tables

The user can use the STORE command to create tables using the data retrieved by a query for his own use. The STORE command creates a table in the user's personal authorization ID and populates the table with the results of the current query. The user can have the data in his own personal tables and then update the tables once a week or whenever convenient.

The Personal Database Facility adds the necessary authorizations required by DQL Language, automatically to personal tables, except when external security is in use. A user who is allowed to use both DQL Language and SQL can access his personal tables from either query mode. A user who is authorized to use SQL only can access another user's personal tables if access privileges have been granted by the owner. Allow users access to personal tables that they require to perform their job functions.

Note: For more information about the GRANT and REVOKE commands for accessing tables, see the *CA Datacom/DB SQL User Guide*.

Here are some considerations for the use of PDB (personal data base) and the STORE command. With these functions, tables are created (by using SQL) into an area specified in the user's profile (this profile information is still used even when external security is in effect for CA Dataquery). The area must be in a database for which the user has both "create" authority and CA Dataquery authority to do maintenance. The area and database should be built separately for each user (or group of users) that are allowed PDB authority, so that these tables are not put into any arbitrary database.

Note: For more information about how to set up a database for SQL use, see the *CA Datacom/DB Database and System Administration Guide*.

You can select portions of tables for a user to access, then use the CA Dataquery Editor to create a view of a portion of a table. The use of views allows users access to the portion of data that they require to perform their job and protects the rest of the data from unnecessary access.

Note: For more information about the use of views, see the *CA Datacom/DB SQL User Guide*.

Assigning Access to Portions of Tables

In SQL Mode, if a user has the need to use only part of a table but does not need to access the entire table, you can create a view of the necessary data and protect the remainder of the table.

You can select portions of tables for a user to access, then have the CA Dataquery Administrator (or whoever you have authorized to use Data Definition Language) use the CA Dataquery Editor to create a view of a portion of a table. The use of views allows users access to the portion of data that they require to perform their job and protects the rest of the data from unnecessary access. See CA Datacom/DB documentation for more information on the use of views.

You can use the CA Dataquery Editor to create a view of a portion of a table. The following is an example of a view created for a user to use to access columns in the CASUPL table. The view states the selected columns names and a search criteria.

Following is an example of an SQL view named SUPPLY:

```
CREATE VIEW SUPPLY
  (SNUM, SNAME, STATUS, CITY)
AS SELECT ALL
  SNUM, SNAME, STATUS, CITY
FROM CASUPL
WHERE STATUS > 10
```

Now when the user accesses the logical table, SUPPLY, the user only accesses the rows of CASUPL when the column status contains a value GT 10.

Note: For more information about Personal Database, see the *CA Dataquery Administrator Guide*.

Using SYNONYM Access

The use of a synonym provides an alternate name for a table. The synonym is a convenience that allows the user to avoid naming both the authorization ID and the table name (authid.tablename) in the query. It has no effect on security. The CREATE SYNONYM command names the authorization ID of the owner and the alternate table name. The other user accesses the table by using the alternate table name in his queries.

Considering CA Datacom System Security

SQL security in CA Datacom/DB can be used in addition to CA Dataquery security to control access to tables. If SQL security is activated at your site, users need to be assigned access to tables before they can access the data in the tables using CA Dataquery. For CA Dataquery SQL Mode, SQL security is the only access control in effect. If your site has an open security system, the security is open to all of your users unless access is specifically prohibited. If your site has a closed security system, the security is closed to all users unless specific access is authorized.

Note: In a closed security system, a user, known to SQL security as USERA, can execute an SQL statement *CREATE TABLE USERB.TAB1* to create a table in the schema USERB. However, USERB would not be able to access this table until USERA grants the privileges through the GRANT command.

It is important that you communicate with your site Database Administrator to gain a clear understanding of the existing security systems and the current CA Datacom Datadictionary profile-codes. You should also make them aware of your needs for establishing a secure CA Dataquery environment. Ongoing communication is imperative, whereby you make your requests known (such as, requesting the creation of new profile-codes) and assure that any changes made within the CA Datacom security environment or in the CA Datacom Datadictionary profile-codes include appropriate plans for maintaining CA Dataquery data integrity and security.

If your site uses CA Ideal, meet with your Database Administrator to ensure that your signon procedures and standards for CA Dataquery security coordinate with those established for the CA Ideal system.

Chapter 5: CA Datacom SQL Security

SQL Security Model

In the SQL Security Model, tables, views, columns, and plans are securable resources. This model includes the automatic granting and revoking of authorizations as tables are created and dropped. It also provides the automatic cascading of revokes and view deletions when authorizations are revoked. SQL security authorizations are established with simple SQL GRANT and REVOKE statements, which may be embedded in programs or executed interactively through the CA Datacom Datadictionary Interactive SQL Service Facility or the CA Dataquery SQL Mode. For more information, see SQL Security Model (see page 285). Plan security is discussed in detail in Plan Security (see page 308).

Note: When an SQL user who created and bound a plan loses an access right to one of the resources used in the plan, the plan is marked invalid. If another user has been executing that plan by using plan security, they find they are then prohibited from using that plan until it has been successfully rebound.

Securing Distributed Access

For databases secured under the SQL Security Model, the Security Facility always validates the authorization of the user at the site (MUF) where the application is executing.

Resource Control

In the SQL Security Model, the creator of the table controls the resource. Anyone who has CATALOG authority for a database can create tables in that database. CATALOG authority is maintained in CA Datacom/DB using an external security product. Tables created by SQL after SQL security is in force for the database, are controlled by the table creator. The creator of a table has ALTER, DROP, and GRANT authority on that table. The table creator grants access authority to users and can optionally give users the ability to grant rights to others.

In addition to the table creator, the Security Administrator also has ALTER, DROP, and GRANT authority on SQL tables. In external CA Datacom/DB security, Security Administrators are defined to the DTADMIN resource class.

Tables do not have a table creator if they were created by an SQL CREATE statement before the SQL Security Model was in force, of if they were created in CA Datacom Datadictionary. In this case, the Security Administrator must issue the first GRANT statement for the table.

SQL plans are securable resources. The user who creates the plan must have all the appropriate access rights for the table(s), view(s), synonym(s), and column(s) used in the plan.

Once a plan is created, the plan owner can grant to others the ability to use the plan even if they do not have the specific access rights required to bind the plan. Plan creators can therefore lend their access rights to other users while executing a specific plan, but without granting those users generic access rights to the resources used by the plan.

The specific access rights and commands involved in using plan security are discussed in Plan Security (see page 308).

Access Rights

A resource owner can use SQL statements to grant access rights to others for the tables, views, columns, or plans controlled by the resource owner. The access rights applicable to tables and views are SELECT, INSERT, UPDATE, DELETE, and ALTER. The only access right applicable to columns is UPDATE. A table, view, or column owner may also allow other users to grant any access they may have on that resource to other users. To permit another individual to grant access to other users, the resource owner must specify the WITH GRANT option when issuing the SQL GRANT statement authorizing that individual access rights.

For SQL plans, the resource owner can grant either "execute" or "bind" authority for a specific plan.

The access rights required to process each SQL statement are listed on SQL Statements and SQL Security Access Rights (see page 300). The rights required to process each CA Datacom/DB command are listed on CA Datacom/DB Commands and SQL Security Access Rights (see page 306).

Naming Accessor IDs in GRANT and REVOKE

Accessors are individuals or groups of individuals who attempt to access data protected by security. When naming an accessor in the SQL GRANT and REVOKE statements, only specify the name of the user. CA Datacom/DB assumes the node to be LOCAL (that is, you are not using distributed processing through CA Datacom STAR) and the type to be USER (that is, an individual identified by a specific user ID) except for the following case.

PUBLIC is a special, reserved accessor name. When used in an SQL GRANT or REVOKE statement, PUBLIC means all individuals and groups of individuals with either a known or an unknown ID.

Validation Process

When the MUF receives a request for access to a CA Datacom/DB database which is defined to use the SQL Security Model, the MUF checks the user's authorizations as defined in the Schema Information Tables (SIT). If the user is authorized for the type of access requested, MUF grants the access.

Activating and Maintaining

Use CA Datacom/DB external security to define CATALOG authorizations to those users who are to be authorized to execute SQL CREATE TABLE statements in the default SQL database or another database which they do not own. For more information, see DBUTLTY and External Security (see page 35).

Issue SQL Statements, from a program or online through the CA Dataquery SQL Mode or CA Datacom Datadictionary Interactive SQL Service Facility, to:

- Grant access rights for accessors of tables and plans.

  Note: For syntax of the plan security versions of the GRANT and REVOKE statements, see Plan Security (see page 308).

- Define views and grant access rights to these views.

Note: For details about the syntax for all statements, see the *CA Datacom/DB SQL User Guide*.

Implementing the SQL Security Model

When defining a database in CA Datacom Datadictionary, you may designate it as secured under the SQL Security Model rules. Choosing this option for a database means that the security for resources in this database is maintained using SQL GRANT and REVOKE statements.

If you choose this option, you are choosing *not* to secure user access for this database in external security. However, we recommend that all security be implemented in external security. A pair of resources is checked in external security either when you catalog or open the database with the SQL security option. This allows the Security Administrator to have control over the use of the SQL security model. The check consists of a pair of resources in the DTSYSTEM resource class as follows:

- cxxname.SQLGRANT.CONTROL.ALLOW
- cxxname.SQLGRANT.CONTROL.DENY

If access is granted to the ALLOW resource and access is denied to the DENY resource, the open or catalog continues. If not, the open or catalog fails with a CA Datacom/DB return code 15(001).

Creating SQL Authorizations

There are two ways to create SQL authorizations:

SQL CREATE Statement

When a user issues a CREATE TABLE or CREATE VIEW SQL statement, CA Datacom/DB automatically creates authorizations. CA Datacom/DB gives the executor of the CREATE TABLE or CREATE VIEW statement all access rights for that table or view (READ, UPDATE, INSERT, DELETE, and ALTER) and marks these authorizations as "grantable," which means that the creator of the table or view may grant those access rights to other users.

SQL GRANT Statement

A user with a grantable access right may execute a GRANT statement to give that access right to some other user. If one user grants an access right to a second user using the WITH GRANT option, the second user may grant the access right to other users.

Table-Level and View-Level Authorizations

At the table/view level, there are access rights named SELECT, DELETE, UPDATE, ALTER, and DELETE. These access rights refer to the authority to execute the corresponding SQL statement against that table or view. For instance, to execute a DELETE statement to delete a row from a table, that user must have the DELETE access right for that table. The ALTER access right applies only to tables.

View Security

This section discusses the implementation of view security for SQL in CA Datacom/DB. Enabling views to secure by name gives greater control because it allows control of access to the precise set of tables, rows, and columns defined by a view.

View Security Overview

View security replaces security authorization checks on the individual tables referenced by a view with a check against the view entity itself. This feature is activated in the external security package. For more information about implementing this choice, see Configuring Your System to Enable View Security (see page 293). The set of access-rights that are securable for a view mirror those securable for a base table.

Whether statements included in a particular plan execute using view security depends upon whether this option was active *during preparation of the plan.* This is true regardless of whether bind-time plan security is being used, that is, when the view access rights of the creator of the plan are checked at bind-time. For those plans that do not use bind-time plan security, view access rights are checked at execution time, but *only* if view security was active at *bind-time.* Otherwise, table-level security is checked.

Whether view security is used for a particular plan is based on the value of the VIEWSEC= Preprocessor plan option. If VIEWSEC= is not specified, whether a plan uses view security is determined by the value of the view-security specification in the SQLOPTION Multi-User startup option. If neither VIEWSEC= nor the view-security specification in SQLOPTION is used, view security is not used for newly bound or rebound plans. For more information on VIEWSEC=, see View Security SQL Preprocessor Option (VIEWSEC=).

View security may be activated or deactivated, intentionally or inadvertently, for existing plans by rebinding them or causing them to auto-rebind. During the rebind, the plan's use of view security is changed using the same set of rules that apply during the initial plan preparation, as described in the preceding paragraph. This means that preexisting plans for which the VIEWSEC option was not specified are changed to use the systemwide default that is in effect at the time of any rebind or auto-rebind. The systemwide default of NO protects these plans from being changed inadvertently.

We do not force rebinds to be performed when this feature is activated. Whether existing plans are rebound is decided by the Security Administrator when the Security Administrator activates view security.

Getting Started

To help ensure that your transition to using view security is smooth, follow these steps:

1. Ensure that your external security package is configured to treat CA Datacom/DB SQL as a *closed system,* that is, all users are barred from accessing any resource if they have not been given explicit access rights. If this precaution is not taken, users can create and use new views against tables even if no access rights have been given.
2. Use the WITH CHECK OPTION clause in the CREATE VIEW statement to specify that all inserts and updates against a view are checked to ensure that the newly inserted or updated row satisfies the view definition.

   Important If you do not use the WITH CHECK OPTION, view security cannot prevent users from adding rows to tables and views that they are not authorized to access. The execution of insert and update statements can be prevented by revoking the INSERT and UPDATE view access rights using external security. Using the WITH CHECK OPTION clause can prevent such access rights violations, however, and that is why we *strongly* recommend that you use the WITH CHECK OPTION clause in any updateable view (that is, single-table, no DISTINCT keyword, and no GROUP BY clause) secured with view security.

3. Add view security authorizations to your external security package. Because you can activate view security on individual plans (see View Security SQL Preprocessor Option (VIEWSEC=) for details), the authorizations you choose to implement can span your entire system or be limited to the set of views referenced by a single application.

   While view security cannot be controlled on a view-by-view basis, it can be controlled at the plan level. This benefits users of plan security and provides a level of control if you want to retain the use of table security for certain applications (or if you want to convert only certain applications to the use of view security). The complexity of security administration can be minimized, however, with a systemwide choice of security method.

   Note: You can retain the table authorizations currently in place, but be aware that for applications using view security, such authorizations are ignored.

   CA Datacom Datadictionary Path reports allow you to see the relationships between tables, views, plans, and programs. You can use these reports to help in the conversion of table authorizations into view authorizations. For details, see Adding View Security Authorizations (see page 291).

4. For the view-security specification in the SQLOPTION Multi-User startup option (in the SYSIN file of your MUF startup JCL), specify YES or NO with regard to whether new and rebound plans are to use view security if they do not have explicit VIEWSEC= Preprocessor specifications. To convert an entire MUF to the use of view security without having to add the VIEWSEC=Y Preprocessor option to existing applications, specify YES for view-security in the SQLOPTION Multi-User startup option and then rebind all of your plans. You can use the SQL Rebind Facility (DBSRFPR) to perform the rebinds if you want to do so. If you do not want existing applications to use view security, either code NO for view-security in the SQLOPTION Multi-User startup option (recommended), or omit the specification. For details, see Adding a Default View Security Specification (see page 293).

5. See Configuring Your System to Enable View Security (see page 293), and follow the instructions.

Adding View Security Authorizations

This section discusses how to determine which views must be secured and shows the format of the security authorizations to add.

Using DDUTILTY to Display Relationships

Alternately, you can use DDUTILTY with the following input to create a report showing the relationships.

```
-DEF PATH,VIEW-USES-TABLES
-DEF TRACE,VIEW.TABLE,VEW-TBL-DEPENDS
-END
-DEF PATH,VIEW-USED-BY-PROGRAMS
-DEF TRACE,VIEW.STATEMENT,STM-VEW-DEPENDS
-DEF TRACE,STATEMENT.PLAN,PLN-STM-CONTAIN
-DEF TRACE,PLAN.PROGRAM,PGM-PLN-USES
-END
-RPT START,VIEW,ALL(PROD),VIEW-USES-TABLES
-END
-RPT START,VIEW,ALL(PROD),VIEW-USED-BY-PROGRAMS
-RPT INDENT,VIEW
-RPT INDENT,PLAN
-RPT INDENT,PROGRAM
-END
-RPT INDENT,PLAN
-RPT INDENT,PROGRAM
-END
```

Name Length Limitations

While reading the resource name formats be aware that the length of each name is limited by the external security package being used. Assuming an 8-character Directory (CXX) name and an external security package that, in an extremely restrictive case, could limit you to 44-byte resource names, the total combined length of the SQL authorization ID and the SQL view name that could be secured could be as short as 28 characters. If, for example, the longest authorization ID in your system is 12 characters long, the longest view name should be 16 characters or less. Check the limits of your external security package and name your views accordingly. Remember that 16 characters of the resource name are reserved for use by SQL (for purposes such as the CXX name).

Access Rights Required

To create a view, you must possess the following access-right under resource class DTUTIL:

```
cxx-name.SVCRE.sql-authid.sql-view-name
```

To drop a view, you need the following access-right under resource class DTUTIL:

```
cxx-name.SVDRP.sql-authid.sql-view-name
```

To read or maintain the data defined by a view, you need the following access-rights under the same table-classes (for example, DXTABLE, DTTABLE) that you are using to secure other SQL resources such as tables.

```
cxx-name.SV.sql-authid.sql-view-name
```

Each resource name is associated with four access-rights: ADD, READ, UPDATE, and DELETE. In concept, this is similar to the method used to grant access-rights to base tables.

Adding a Default View Security Specification

To add a default view security specification to the SYSIN parameters of your MUF startup JCL, add a comma followed by the word YES or NO to the SQLOPTION statement so that the new specification occupies the fifth position in the comma-separated list. For example:

```
SQLOPTION YES,17,DATACOM,120,YES
```

The first YES specifies that SQL is to be enabled for use. The 17 specifies that the SQL Temporary Table Manager is in database ID 17. The DATACOM specifies the default for the SQLMODE= value in the SQL Preprocessor plan option. The 120 is the default LUW TIMEOUT specification. The next parameter, YES, specifies that view security is to be used for all plans that do not have an explicit VIEWSEC= specification.

Note: For more information, see the *CA Datacom/DB Database* and *System Administration Guide*.

Configuring Your System to Enable View Security

The following information is designed for Security Administrators familiar with basic external security concepts related to CA Datacom/DB.

View security is implemented in level 04 or higher security. This level is defined in the same way as the other security levels. To enable this level, the user ID which is associated with the MUF submission must be allowed access to DTSYSTEM resource ACTIVATE.LEVEL04.PASS and denied access to DTSYSTEM resource ACTIVATE.LEVEL04.FAIL.

This feature is enabled based on denial of access to resources to ensure that pre-existing access authorizations that are already in place on your system do not inadvertently enable the feature.

If level 04 or higher security is in place, an additional DTSYSTEM resource (cxxname.SV.ENABLE) is checked at MUF startup. If access is denied to this resource, views can be secured externally. An additional DB00220I message is printed indicating VIEW security is in place.

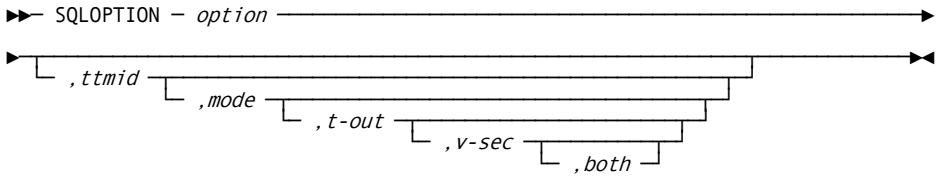
The following additional edits are performed at MUF startup if YES is specified for the SQLOPTION Multi-User startup option view-security choice that sets the default for the VIEWSEC= Preprocessor option:

1. Level 04 security is checked to make certain it is in place.
2. A DTSYSTEM resource name of cxxname.SV.DEFAULT is checked. Access is denied to this resource if default YES is specified. This edit prevents views from being inadvertently changed to use view security.

If either edit fails MUF does not enable but instead receives a DB00205E error with an error code of 1092.

SQLOPTION Multi-User Startup Option

The view-security specification in the SQLOPTION Multi-User startup option is used to specify the default for the SQL VIEWSEC= Preprocessor option (see View Security SQL Preprocessor Option (VIEWSEC=)).



option

(Required) Indicate if SQL is generated for this MUF.

Valid Entries:

YES or NO

Default Value:

(No default)

,ttmid

(Optional) Specify the CA Datacom/DB database ID used for the SQL Temporary Table Manager area. Allowed only if *option* (see previous) is set to YES.

Valid Entries:

The DATACOM-ID of the database

Default Value:

17

,mode

(Optional) Specify the edit mode in which SQL programs are processed. You must specify the above parameters before you can specify this parameter.

Value	Meaning
ANSI	All SQL statements must be coded according to ANSI standards. Specifying ANSI overrides any specification for the SQLMODE= Preprocessor option.
DATACOM	CA Datacom/DB extensions to the ANSI standards are allowed in SQL statements. When you specify DATACOM, the SQLMODE= Preprocessor option can be used to specify ANSI, FIPS, or DB2 on a program-by-program basis.
FIPS	All SQL statements must be coded according to Federal Information Processing Standards (FIPS). Specifying FIPS overrides what you specify for the SQLMODE= Preprocessor option.

Valid Entries:

ANSI, DATACOM, or FIPS

Default Value:

DATACOM

,t-out

(Optional) Specify the time-out value in minutes after which inactive SQL logical units of work are automatically closed in a CICS system. SQL Preprocessor option ISOLEVEL= information includes details about logical units of work in an SQL environment. You must specify the above parameters before you can specify this parameter.

If you code zero, no automatic close occurs.

Valid Entries:

0—1440

Default Value:

120

,v-sec

(Optional) Specify the default view security value for the SQL Preprocessor option VIEWSEC= (see View Security SQL Preprocessor Option (VIEWSEC=)). Specify YES to indicate that view security is to be used during the execution of newly prepared and newly rebound plans.

Specify NO to indicate that view security is not to be used during the execution of newly prepared and newly rebound plans.

Note: This choice of security method is made at prepare time rather than during execution. A choice of YES is rejected if view security has not been activated for the MUF using external security.

Important Subsequently rebound plans (rebound explicitly or automatically) that do not have an explicit view security specification are caused by the value of the SQLOPTION view-security option to change security methods, if necessary, to match the specification. Be aware, therefore, that the security method used by existing plans can be changed *intentionally or inadvertently* in this way.

Valid Entries:

YES or NO

Default Value:

NO

,both

(Optional) Specify whether both update and read-only cursors are allowed within a plan. YES indicates both are allowed. NO indicates either an update or read-only cursor is allowed.

Valid Entries:

YES or NO

Default Value:

NO

View Security SQL Preprocessor Option (VIEWSEC=)

The VIEWSEC= Preprocessor option is used to specify whether view security is to be used during the execution of newly prepared and newly rebound plans.

VIEWSEC=

Whether view security is used for a particular plan is based on the value of the VIEWSEC= Preprocessor plan option. If VIEWSEC= is not specified, whether a plan uses view security is determined by the value of the view-security specification in the SQLOPTION Multi-User startup option. If neither VIEWSEC= nor the view-security specification in SQLOPTION is used, view security is not used for newly bound or rebound plans.

Specify Y to indicate that view security is to be used during the execution of newly prepared and newly rebound plans.

Specify N to indicate that view security is not to be used during the execution of newly prepared and newly rebound plans.

Note: The default for the VIEWSEC= Preprocessor option is the value of the view-security option in the SQLOPTION Multi-User startup option (see SQLOPTION Multi-User Startup Option for more information) or N if no default was specified.

Also note, the choice of security method is made at prepare-time rather than during execution. A choice of Y is rejected if view security has not been activated for the MUF using external security.

Valid Entries:

Y or N

Default Value:

Value of the view-security specification in the SQLOPTION Multi-User startup option, which itself defaults to N.

Important! Subsequently rebound plans (rebound explicitly or automatically) that do not have an explicit view security specification are caused by the value of the SQLOPTION view-security option to change security methods, if necessary, to match the specification. Be aware, therefore, that the security method used by existing plans can be changed *intentionally or inadvertently* in this way.

Synonyms

Access rights are not definable for synonyms. If an SQL statement contains a synonym, CA Datacom/DB checks the authorizations for the table or view it represents.

Column-Level Authorizations

The only column-level access right is the UPDATE right. For example, if you want GEORGE to be able to read all of the table but to only be able to update the DESCRIPTION column, grant GEORGE the SELECT access right to the table and the UPDATE access right for the DESCRIPTION column.

Granting a table-level UPDATE access right overrides any column-level UPDATE access rights, as in the following example:

SAM is granted the UPDATE access right on only the DESCRIPTION column by the creator of the table, ED. ED also grants the table-level UPDATE access right, with grant option, to SALLY. If SALLY then grants UPDATE at the table-level to SAM, SAM now has both the table-level UPDATE access right and a column-level UPDATE access right on one column of the table. The table-level access right takes precedence, and he may update any column. However, if SALLY later revokes the table-level access right from SAM, his authorization reverts to the one-column-only status granted to him by ED.

Plan Authorizations

For information about plan authorizations, see Plan Security (see page 308).

Authorization for PUBLIC Access

A creator of a table or view may grant access rights on that object to all users, including unknown users, by granting them to PUBLIC, a special reserved word meaning "all accessors, including those defined later."

CATALOG Authorization

To issue a CREATE TABLE statement, a user must have either the CATALOG access right or Ownership status for the database to which the new table belongs. If the user does not specify an IN AREA clause with the CREATE TABLE statement, the table is created in the default area specified at Multi-User startup and the user must have CATALOG access for the database containing this area.

Note: For more information, see the Multi-User startup option SQLDEFAULT in the *CA Datacom/DB Database and System Administration Guide.*

With external security, the owner of a database is a user with access to the special system.DB00nnn.999.CATALOG resource in the DTUTIL resource class. For more information, see DBUTLTY and External Security (see page 35).

Global Ownership

Only a Global Owner can issue the CREATE SCHEMA statement. A Global Owner owns all resources. Therefore, a Global Owner can DROP any SYNONYM, VIEW, or TABLE and may GRANT or REVOKE any access rights.

With external security, a Global Owner is a user who is authorized access to the system.DB resource in the DTADMIN resource class. For more information, see DTADMIN (see page 32).

Deleting Access Rights

SQL Authorizations are deleted:

- When a user executes a REVOKE statement to cancel an authorization previously granted with a GRANT statement.
- When a table or view is dropped.
- When the accessor who bound a plan loses the access rights to one of the resources used in the plan.

Cascading of REVOKE and DROP

Issuing a REVOKE statement or dropping a table or view may have cascading effects on other authorizations. If a user has the authority to grant access rights to other users, revoking access rights of that user to a table or view automatically revokes any access rights to that table or view which that user had granted to other users. This cascading action ensures that all authorizations which depended on the original authorization are also revoked. There are also situations where views may be dropped as the result of a REVOKE statement. For more information, see Data Control Language (DCL) Operations (see page 305).

Execute rights for a plan are dropped if the "binder" of the plan loses (by the use of the SQL REVOKE statement) access to a resource used in the plan. This is not true, however, if the access is derived from the use of external security.

Binding of GRANT and REVOKE Statements

When an SQL Data Manipulation Language (DML) statement is compiled, the access rights needed to execute that statement are determined and put into a list in the compiled form of the statement. The objects mentioned in the statement must exist at compile time.

Data Control Language (DCL) statements (such as GRANT and REVOKE) are implemented like Data Definition Language (DDL) statements. The objects mentioned in the statement must exist at execution time but are not required to exist at compile time. This allows a GRANT statement to be in the same module with the CREATE TABLE statement when both refer to the same table.

Required Access Rights

The tables which follow detail the SQL Security Model access rights which a user must have to issue each of the SQL statements and CA Datacom/DB commands and any effects the statement or command has on security.

SQL Statements and SQL Security Access Rights

The CA Datacom/DB SQL statements and SQL security access rights are categorized in this section as follows:

- Data Manipulation Language (DML) Cursor Operations
- Data Manipulation Language (DML) Non-cursor Operations
- Data Manipulation Language (DML) Transaction Level Operations
- Data Definition Language (DDL) Operations
- Data Control Language (DCL) Operations

Data Manipulation Language (DML) Cursor Operations

Statement	Authorization Required	Authorization Implications
CLOSE	None	None
DECLARE CURSOR	None	None
DELETE	DELETE	None
FETCH	None (CA Datacom/DB checks access rights at cursor OPEN.)	None

Statement	Authorization Required	Authorization Implications
OPEN	SELECT access for each table or view specified in the SELECT statement (or PUBLIC must have the SELECT access right for those tables and/or views).	None
UPDATE	UPDATE access for the table or view specified in the statement (or PUBLIC must have the UPDATE access right for that table or view).	None

Data Manipulation Language (DML) Non-cursor Operations

Statement	Authorization Required	Authorization Implications
DELETE	DELETE access for the table or view specified in the statement (or PUBLIC must have the DELETE access right for that table or view). SELECT access for any table or view specified in the WHERE clause (or PUBLIC must have the SELECT access right for that table or view).	None
INSERT	INSERT access for the table or view specified in the statement (or PUBLIC must have the INSERT access right for that table or view). SELECT access for any table or view specified in the WHERE clause (or PUBLIC must have the SELECT access right for that table or view).	None
SELECT INTO	SELECT access for each table or view specified in the statement (or PUBLIC must have the SELECT access right for those tables and/or views).	None

Statement	Authorization Required	Authorization Implications
UPDATE	UPDATE access for the table or view specified in the statement or column-level UPDATE access for all of the columns in the Set List (or PUBLIC must have the required UPDATE access rights). SELECT access for any table or view specified in the WHERE clause (or PUBLIC must have the SELECT access right for that table or view).	None

Data Manipulation Language (DML) Transaction Level Operations

Statement	Authorization Required	Authorization Implications
COMMIT WORK	None	None
LOCK TABLE	SELECT access to the table for a shared lock. UPDATE access to the table for an exclusive lock.	None
ROLLBACK WORK	None	None

Data Definition Language (DDL) Operations

Statement	Authorization Required	Authorization Implications
COMMENT ON	Creator of the view or table.	None
ALTER TABLE	ALTER access for the table. *	None
CREATE INDEX	INDEX access for the table being indexed.	None

Statement	Authorization Required	Authorization Implications
CREATE SCHEMA	Accessor must be a Global Owner and have the access rights required to execute statements (such as CREATE TABLE) included in the CREATE SCHEMA statement.	The only security effects are those of the statements included in the CREATE SCHEMA statement.
CREATE SYNONYM	None	The owner of the synonym (the ID executing the CREATE VIEW statement) is recorded in CA Datacom Datadictionary.
CREATE TABLE	CATALOG access for the database in which the table is created. (CATALOG rights are granted with the Online Security Maintenance Facility.)	The user is the owner of the created table with grantable SELECT, UPDATE, INSERT, DELETE, and ALTER access rights.

Statement	Authorization Required	Authorization Implications
CREATE VIEW	SELECT access for each table or view in the statement (or PUBLIC must have the SELECT access right for that table or view).	The creator of the view always acquires the SELECT access right on the view. The SELECT access right is grantable only if the creator has the grantable SELECT access right on every table or view identified in the first FROM clause of the SELECT statement of the view. The creator also acquires any other access right that can apply to the view and that is an access right which the creator has been granted on the tables or views identified in the first FROM clause of the SELECT statement of the view. The access right is grantable only if all of the access rights from which it is derived are grantable. No column-level access rights are automatically granted. If the accessor has UPDATE access rights at only the column level for a table or view in the subselect, the UPDATE access right is not inherited for the view.
DROP INDEX	INDEX access for the table being indexed.	None
DROP SYNONYM	Creator of the synonym or a Global Owner. *	None
DROP TABLE	Creator of the table or owner of the database containing the table. *	All owner definitions and all authorizations involving the table are revoked.
DROP VIEW	Creator of the view or a Global Owner. *	All authorizations on the view are revoked.

* CA Datacom/DB does not process a DROP or ALTER statement and returns a -118 SQL return code when the CA Datacom Datadictionary entity-occurrence definition of the table, view, or synonym specified is protected with a password or a Lock Level 1 or 2. For more information about passwords and lock levels, see the CA Datacom Datadictionary documentation.

Data Control Language (DCL) Operations

Statement	Authorization Required	Authorization Implications
GRANT	If granting a table-level access right, a user must have that same access right with the grant option. If granting a column-level access right, a user must have that access right with grant option, or the corresponding table-level access right with grant option. A Global Owner may execute any GRANT statement.	The requested authorizations are established.

Statement	Authorization Required	Authorization Implications
REVOKE	To REVOKE access rights from another user, the user must have granted that other user the access rights. A Global Owner may REVOKE any user's access rights to any resource.	If the user, whose access right is revoked, has granted the access right to someone else, that access right is also revoked, which may cause further revokes, and so on. CA Datacom/DB revokes the entire tree of access rights depending on the original revoked access right. When an access right is revoked, CA Datacom/DB examines all views created by that user to determine whether not having the access right would prevent that view from being created now. If so, CA Datacom/DB drops the view. Since, when a view is created, the creator of the view is automatically granted access rights based on the access rights they have on the underlying tables and views, whenever an access right on a table or view is revoked, CA Datacom/DB examines all views created by the user on that table or view to determine if any of the access rights that were automatically granted would not now be granted because of the revoke. If so, CA Datacom/DB revokes them.

CA Datacom/DB Commands and SQL Security Access Rights

Command	Authorization	Function
ADDIT	INSERT	Add Record
CNTFL/CNTTB	SELECT	Count for Table
CNTKR	SELECT	Count for Key Value Range
CNTKY	SELECT	Count for Equal Key Value
DELET	DELETE	Delete Record
GETIT	SELECT	Retrieve Next Sequential Record
GETPS	SELECT	Get Next Physical Sequential Record

Command	Authorization	Function
GSETL	SELECT	Set to Starting Key Value
GSETP	SELECT	Set Physical Sequential Record Processing
LOCBR	SELECT	Locate Backwards
LOCKG	SELECT	Locate Key Equal or Higher
LOCKI	SELECT	Test for Logical Intersections of Two Keys
LOCKL	SELECT	Locate Key Value Equal or Lower
LOCKR	SELECT	Locate a Record in a Specified Range
LOCKX	SELECT	Locate Key Value Exact
LOCKY	SELECT	Locate Key Value Equal or Higher
LOCNE	SELECT	Locate Next Equal Key Value
LOCNK	SELECT	Locate Next Key Value
LOCNR	SELECT	Locate Next Record in Specified Range
LOCNX	SELECT	Locate Next
REDBR/RDUBR	SELECT	Read Backwards
REDID/RDUID	SELECT	Read Record by ID
REDKG/RDUKG	SELECT	Read Record Greater Than or Equal to Key
REDKL/RDUKL	SELECT	Read Key Less Than or Equal to Key
REDKR/RDUKR	SELECT	Read Record in a Specified Range
REDKX/RDUKX	SELECT	Read Key Exact
REDKY/RDUKY	SELECT	Read Key Exact
REDLE/RDULE	SELECT	Read Located Entry
REDNE/RDUNE	SELECT	Read Next Equal Key Value
REDNK/RDUNK	SELECT	Read Record with the Next Sequential Key Value
REDNR/RDUNR	SELECT	Read the Next Record in a Specified Range
REDNX/RDUNX	SELECT	Read Next
SELCN	SELECT	Continue Set Record Selection

Command	Authorization	Function
SELFR	SELECT	Select Set - Return First Record
SELNR	SELECT	Select Next Record
SELPR	SELECT	Release Set
SELSM	SELECT	Select Same Record
SELST	SELECT	Stop Set Record Selection
UPDAT	UPDATE	Update Record

Plan Security

SQL plans are securable. That is, with plan security you can create a plan such that, in order to execute the plan, an accessor ID must have the plan EXECUTE privilege for that plan. The plan EXECUTE privilege can be granted with the GRANT statement and revoked with the REVOKE statement. For more information, see Plan EXECUTE and Plan BIND Privileges (see page 310).

Plan security allows the Security Administrator to limit what can be accessed by a given interactive SQL product user while allowing that same user access to the restricted tables while executing the *trusted* plan.

After the system determines that an accessor ID has the authority to execute a plan, no further privilege-checking is done. However, when the plan was created, the *binder* of the plan was checked to ensure that the privileges required to execute the plan existed. Therefore, the executor of such a plan temporarily assumes the privileges of the binder of the plan, and it is up to the binder to ensure that the executor does not violate security.

There is no special privilege required to create a plan, but the ability to create a plan which uses the *binder's* privileges (instead of the executor's) is controlled by the use of the CHECKWHO=BINDER plan option. To use CHECKWHO=BINDER, you need the system-level CHECKBINDER privilege. For more information, see Plan Options in Plan Security (see page 312) and CHECKBINDER System Privilege (see page 314).

If the plan is not secured, security works as follows:

- Anyone can execute the plan (privileges are checked using the accessor ID of the executor of the plan at execution time),
- Anyone can preprocess the plan, and
- Anyone can rebind or delete the plan.

If the plan is secured, however, users must possess the proper privileges before they can execute, preprocess, rebind, or delete the plan.

Note: External security is the preferred method for securing all SQL resources.

Plan security authorizations (CHECKBINDER, PLAN EXECUTE, PLAN BIND) are checked using the following criteria. If any external security path is active, external security is checked. Otherwise, SQL GRANT/REVOKE security is checked. If neither security method is active but an attempt is made to use SQL plan security anyway, the authorization attempt is rejected as if security had been active and the user was unauthorized.

Externalization of Plan Security

Users of CA ACF2, CA Top Secret, and RACF can take advantage of SQL plan security by using statements (in their own security packages) equivalent to the SQL GRANT and REVOKE statements to control the plan EXECUTE, plan BIND, and system level CHECKBINDER privileges. For more information, see Externalization of Plan Security.

Controlling Access to Plans

Access to plans is controlled by using a:

- Plan security GRANT statement (see following),
- Plan security REVOKE statement (see following), and a
- Plan option, CHECKPLAN=.

  Note: Three other plan options, CHECKWHEN=, CHECKWHO=, and SAVEPLANSEC= are also used in plan security.

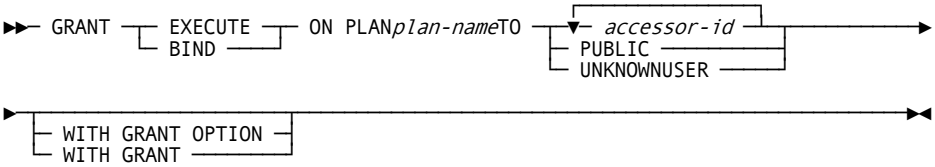
  For more information about CHECKPLAN= and the other three plan security options, see Plan Options in Plan Security (see page 312).

Plan EXECUTE and Plan BIND Privileges

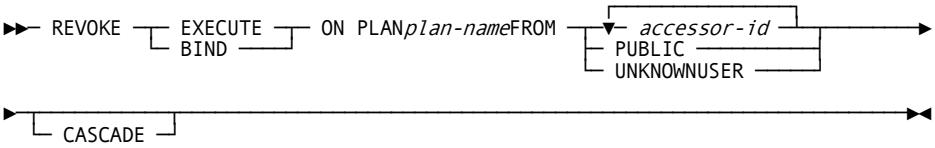
Plan EXECUTE and plan BIND privileges can be granted and revoked by using the plan security versions of the GRANT and REVOKE statements.

Note: To grant a plan privilege you must possess that privilege WITH GRANT OPTION or be a Global Owner. To revoke a plan privilege you must have granted the privilege or be a Global Owner. See Global Ownership (see page 299).

Here is the syntax diagram for the plan security version of the GRANT statement.



Here is the syntax diagram for the plan security version of the REVOKE statement.



privilege-name

Specifying EXECUTE for privilege-name grants or revokes a plan EXECUTE privilege. The plan EXECUTE privilege allows an accessor ID to execute the plan.

Specifying BIND for privilege-name grants or revokes the plan BIND privilege. The plan BIND privilege is required for an accessor ID to create, rebind, or delete a plan.

The creator of a plan is automatically granted the EXECUTE and BIND privileges for that plan. The EXECUTE and BIND privileges are ignored by the SQL Manager if the plan privileges are checked externally. For more information, see Using External Security for CA Datacom.

ON PLAN *plan-name*

For *plan-name*, specify the name of the plan to or from which the plan EXECUTE or plan BIND privilege is to be granted or revoked.

accessor-id

Specify the accessor ID of one or more users to whom you are granting or revoking privileges (you can only use a REVOKE statement to revoke privileges that were granted with a GRANT statement). Note that an accessor ID is a *user's* ID, not a schema authid. When using GRANT, do not specify your own accessor ID (you cannot grant privileges to yourself). If listing more than one accessor ID, separate them with commas.

PUBLIC

Specify PUBLIC when you are granting or revoking the specified privileges to or from all users. A new user automatically has any privileges previously granted to the public.

UNKNOWNUSER

Specify UNKNOWNUSER when you are granting or revoking the specified privileges to or from users whose identities cannot be determined by the CA Datacom/DB Security Facility.

WITH GRANT OPTION

(Optional) Specify this option if you want the user to whom you have granted the privilege to be able to grant it to another user. The WITH GRANT OPTION cannot be used with PUBLIC.

WITH GRANT

Specify WITH GRANT if you want the user to whom you have granted the privilege to be able to grant it to another user. WITH GRANT cannot be used with PUBLIC or with UNKNOWNUSER.

CASCADE

(Optional) If CASCADE is specified, any other dependent privileges that have been granted to others (through the GRANT statement) are also revoked. If a REVOKE is issued without CASCADE and the grantee granted privileges to other users, the REVOKE is not permitted. The CASCADE option of REVOKE does not block the cascading effect of a revoke but operates instead as a fail-safe device. Specifying CASCADE simply acknowledges your understanding that there are cascading effects.

You can find more information related to GRANT and REVOKE in Cascading of REVOKE and DROP (see page 299) and Binding of GRANT and REVOKE Statements (see page 300). For still more information about the GRANT and REVOKE statements, see the *CA Datacom/DB SQL User Guide*.

Plan Options in Plan Security

This section describes the four plan options used in plan security: CHECKPLAN=, CHECKWHEN=, CHECKWHO=, and SAVEPLANSEC=.

Following is a chart showing which combinations of CHECKWHO=, CHECKWHEN=, and CHECKPLAN= are valid. Refer to this chart when studying the descriptions that begin on the following page.

Plan Options	**Values**							
CHECKWHO (B=BINDER, A=ACCESSOR)	B	B	B	B	A	A	A	A
CHECKWHEN (B=BIND, E=EXECUTE)	B	B	E	E	B	B	E	E
CHECKPLAN (N=NO, Y=YES)	N	Y	N	Y	N	Y	N	Y
ALLOWABLE COMBINATION? (Y=YES, 1/2/3 see below)	1	Y	1	2	3	3	Y	Y

REASON CODES

1. Not allowed because with plan-level security off, anyone could run this plan, and the executor's table-level privileges would not be checked.

2. Not currently supported.

3. Not allowed because SQL does not know at bind-time whom the executors are going to be.

Description of Options

CHECKPLAN=

This plan option allows the creator of a plan to specify whether that plan is to be secured.

If CHECKPLAN=Y, any accessor ID which attempts to execute the plan must have the PLAN EXECUTE privilege for that plan.

If CHECKPLAN=N, any accessor ID can execute the plan (table-level privileges, however, are still checked).

For the chart showing the valid combinations of CHECKPLAN=, CHECKWHEN=, and CHECKWHO=, see Plan Options in Plan Security (see page 312).

Valid Entries:

Y or N

Default Value:

CHECKPLAN=N is the default only if the CHECKPLAN= parameter in the PLANSEC Multi-User startup option was *not* specified. If the CHECKPLAN= parameter in PLANSEC *was* specified, its value is the default here.

Note: For more information about Multi-User startup options, see the *CA Datacom/DB Database and System Administration Guide*.

CHECKWHEN=

Specifies whether table-level privileges are to be checked at bind or runtime.

If CHECKWHEN=BIND, then CHECKWHO=BINDER must be specified (it is impossible for SQL to know all potential executors). Similarly, if CHECKWHO=ACCESSOR, then CHECKWHEN=EXECUTE must be specified.

For the chart showing the valid combinations of CHECKPLAN=, CHECKWHEN=, and CHECKWHO=, see Plan Options in Plan Security (see page 312).

Valid Entries:

BIND or EXECUTE

Default Value:

EXECUTE is the default only if the CHECKWHEN= parameter in the PLANSEC Multi-User startup option was *not* specified. If CHECKWHEN= in PLANSEC *was* specified, its value is the default here.

Note: For more information about Multi-User startup options, see the *CA Datacom/DB Database and System Administration Guide*.

CHECKWHO=

Used to specify whether table-level privileges are checked at bind or execute time, and whether the access rights of the binder or the executor are checked. If CHECKWHO=BINDER, the only privilege needed by an accessor ID to run that plan is the PLAN EXECUTE privilege (all table-level privileges required to execute the plan are checked using the binder's accessor-ID). Since the CHECKWHO=BINDER type of plan allows the binder to effectively grant temporary privileges to accessors who use the plan, the ability to create CHECKWHO=BINDER plans must be strictly controlled. To create a CHECKWHO=BINDER plan, you must possess the CHECKBINDER system privilege. For information about the granting and revoking of the CHECKBINDER system privilege, see CHECKBINDER System Privilege (see page 314).

Because it is impossible for SQL to know all potential executors, specify CHECKWHO=BINDER if CHECKWHEN=BIND and CHECKWHEN=EXECUTE if CHECKWHO=ACCESSOR.

For the chart showing the valid combinations of CHECKPLAN=, CHECKWHEN=, and CHECKWHO= earlier in this topic.

Valid Entries:

ACCESSOR or BINDER

Default Value:

ACCESSOR is the default only if the CHECKWHO= parameter in the PLANSEC Multi-User startup option was *not* specified. If the CHECKWHO= parameter in PLANSEC *was* specified, its value is the default here.

Note: For more information about Multi-User startup options, see the *CA Datacom/DB Database and System Administration Guide*.

SAVEPLANSEC=

Use this option to specify whether to drop or not to drop security privileges granted on a PLAN when a program is re-preprocessed.

SAVEPLANSEC=Y means PLAN privileges are not dropped and therefore do not have to be regranted after re-preprocessing a program.

SAVEPLANSEC=N means PLAN privileges are dropped (revoked).

Valid Entries:

Y or N

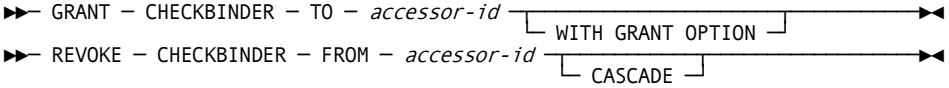
Default Value:

N

CHECKBINDER System Privilege

Anyone can create a plan, but the ability to create a plan which uses the *binder's* privileges instead of the executor's is controlled by the use of the CHECKWHO=BINDER plan option, for which you need system-level CHECKBINDER privilege.

The following diagram shows how the CHECKBINDER privilege is granted and revoked in plan security.



To grant the CHECKBINDER privilege, the grantor must hold the privilege WITH GRANT OPTION or be a Global Owner. To revoke the CHECKBINDER privilege, you must have granted it to the revokee or be a Global Owner. For more information about Global Owners, see Global Ownership (see page 299).