CA Tape Encryption

CA Graphical Management Interface (CA GMI) User Guide

Release 14.5.00

CA Technologies Product References

This document references the following CA Technologies products:

- CA Tape Encryption
- CA Tape Encryption Key Manager

Contact CA Technologies

Contact CA Support

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

- 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

Provide Feedback

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

If you would like 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: Using the CA Tape Encryption GUI 7

Chapter 2: Auditing CA Tape Encryption 31

Chapter 3: Verifying CA Tape Encryption 61

Chapter 1: Using the CA Tape Encryption GUI

This section contains the following topics:

CA GMI

CA GMI is the GUI that allows you to view and manage information about storage management product activity, including CA Tape Encryption. It consists of the Windows Client GUI, which interfaces with a z/OS server component to allow access to basic z/OS server functions.

CA GMI is included with many CA products. If you already have one of the following products installed, you do **not** need to install the CA GMI again for CA Tape Encryption.

- CA 1
- CA ASTEX
- CA SRM
- CA CREWS
- CA Disk
- CA IDMS/DB
- CA MasterCat
- CA TLMS
- CA Vantage
- CA Vtape

For more information about using CA GMI, see the *CA Vantage Windows Client User* Guide.

Note: To review the most current list of products that have recently included CA GMI, select “SupportConnect” at http://ca.com/support http://www.ca.com/support \o \t _blank, then the “Product Home Pages” option, and select the product “CA Vantage Storage Resource Manager GMI.”

Standard CA GMI Features

CA GMI provides a rich set of standard features for working with all of these products. These features include the following:

- Ability to connect to several z/OS hosts at the same time, with separate views for each host, or all hosts consolidated into a single view. Access to objects and actions on each z/OS host is controlled by the z/OS security system on that host (CA ACF2, CA Top Secret, or IBM Security Server RACF)
- Table views of all data, customizable with the ease of point-and-click
- Graphical views of any numeric data, easily customized, with a wide range of two-dimensional and three-dimensional features
- Filtering and sorting on any field
- Aggregate functions (total, average, min and max)
- Scaling (KB, MB, GB, and so on) and color coding features
- Drill-down feature to zoom to related object data
- Wizards for simple or complex summaries
- Reporting features for customized and printed reports
- Multiple output formats, including:
  - Web page
  - Email
  - PDF document
  - Excel
  - Microsoft Access Database (MDB)
- Schedulers for producing and sending report output on a regular basis
- JCL management (edit, model, drag and drop, substitute, submit, schedule)

z/OS Server Objects

The z/OS server portion of CA GMI performs the data retrieval and actions that you request from the Windows Client. It does this for the objects provided by CA Tape Encryption, as well as for the following basic storage management objects:

- Volumes (space usage and other attributes)
- Storage Groups (space usage and other attributes)
- DFSMS Constructs (all attributes)
- Catalogs (locations, relationships, entries and space usage)
- z/OS System Resources (APF list, Link list, and so on)
- System Activity (Message Log, Mailbox, System Parameters, Operator Commands and others)
- Analysis Tools (memory usage, object dictionary and component analysis)

Install and Configure CA GMI

CA GMI has two components:

z/OS Server

Installed on the mainframe from a tape

CA GMI Windows Client GUI (Windows Client)

Installed on the PC from a CD

Installation

In order to use CA GMI you must install and configure both the z/OS Server and the Windows Client components.

Note: If you have already installed CA GMI components for one of the other CA GMI products, there is no need to install the components again. If you are installing them for the first time, ensure that you have received the proper installation materials for both components. If you do not have them, contact Technical Support at http://ca.com/support http://www.ca.com/support \t _blank.

To install and configure both components of GMI

Note: System software and hardware requirements for both components of GMI can be found in the *CA Vantage Storage Resource Manager Installation at a Glance* poster. You can access the CA Vantage documentation set from the product CD, download copies from http://ca.com/support http://www.ca.com/support \t _blank, or you can install the Windows Client first (with no configuration) and then access the CA Vantage documentation set as explained in the section How You Use the Windows Client GUI.

1. Install the z/OS server as described in the *CA Vantage Installation Guide* guide.

   The z/OS server is installed on your z/OS system.

   Install the Windows Client and configure the parts of the z/OS server that are common to all GMI products as described in the chapter “Configure GMI” in the *CA Vantage User Guide*.

   The Windows Client is installed on your PC and common GMI parts of the z/OS server are configured on your z/OS system.

2. Configure the parts of the z/OS server that are specific to CA Tape Encryption according to the chapter “Configure GMI Qualified Products” in the *CA Vantage User Guide*.

   CA Tape Encryption objects are defined for retrieving CA Tape Encryption object data by the Windows Client.

3. Start the Windows Client according to the section Start the Windows Client GUI in the chapter “Auditing CA Tape Encryption.”

   The Windows Client is up and running on your PC.

4. Define z/OS hosts as described in the section Define the z/OS Host in the chapter “Auditing CA Tape Encryption.”

   At least one z/OS host is defined in your Host List.

5. Connect the Windows Client to a z/O host and login as described in the section Log in to the z/OS Host in the chapter “Auditing CA Tape Encryption.”

   Your Windows Client is connected and logged in to a z/OS host.

6. Define the Windows Client data collection mode as described in the section Data Collection Modes in the chapter “Auditing CA Tape Encryption.”

   Object data is automatically displayed in the object view when you open an object.

How You Use the CA Vantage Windows Client GUI

The following sections show you how to use the CA GMI with CA Tape Encryption.

Note: For more specific details about the many features in the Windows Client, consult the Windows Client online Help system or the *CA Vantage Windows Client User Guide*.

After you install the Windows Client you can access the CA Vantage documentation set by following these steps:

1. Click Start, Programs, CA, CA Storage Resource Manager, Documentation, and then select Manuals - z OS, or click Help on the menu bar at the top of the Main Window of the Windows Client, then select Manuals - z/OS.

   Either option will result in the CA Vantage Bookshelf being displayed in Acrobat Reader.

2. Click the Search All Guides button to have Acrobat Reader search all the guides in the list for a particular word or phrase, or click one of the manuals in the table to view it.

You can access the Windows Client online Help system by clicking the Help icon in the toolbar at the top or bottom of most of the windows or dialogs displayed by the Windows Client.

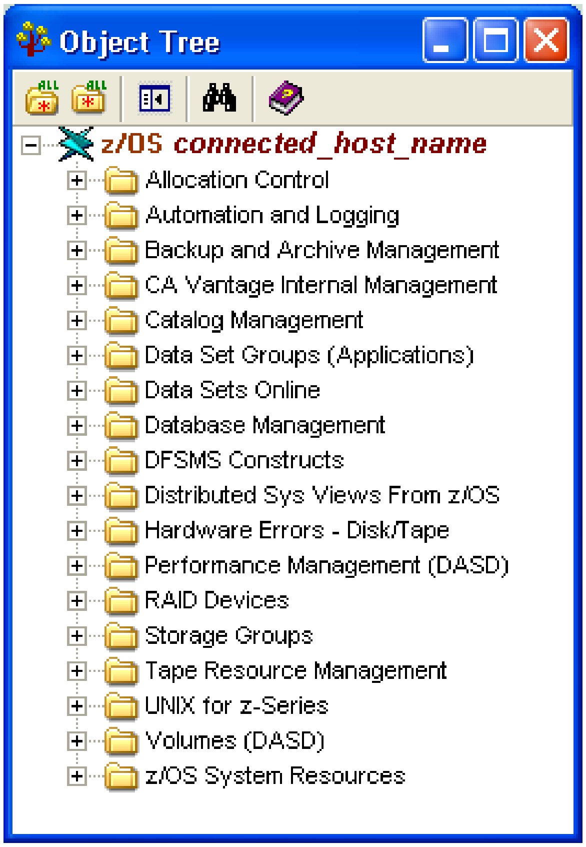
Accessing CA Tape Encryption Objects from the Windows Client

All CA Tape Encryption objects are included in the Tape Resource Management folder that is visible when the z/OS Object Tree is opened.

To access CA Tape Encryption objects, perform the following steps:

1. Open the Windows Client and connect to the z/OS host.
2. In the toolbar at the top of the Main Window of the Windows Client, click the Object Tree icon to open the z/OS Object Tree.

   The z/OS Object Tree opens, as shown in the following example:

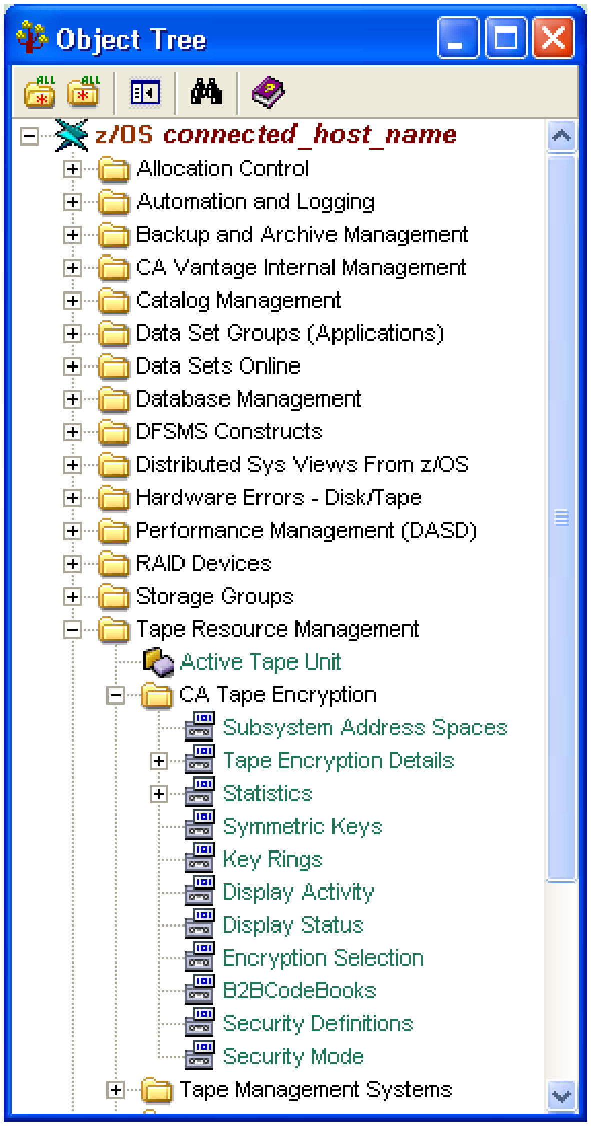


Object Tree

z/OS connected_host_name
- Allocation Control
- Automation and Logging
- Backup and Archive Management
- CA Vantage Internal Management
- Catalog Management
- Data Set Groups (Applications)
- Data Sets Online
- Database Management
- DFSMS Constructs
- Distributed Sys Views From z/OS
- Hardware Errors - Disk/Tape
- Performance Management (DASD)
- RAID Devices
- Storage Groups
- Tape Resource Management
- UNIX for z-Series
- Volumes (DASD)
- z/OS System Resources

3. Expand the Tape Resource Management folder.

4. Double click the **CA Tape Encryption** folder to expand the tree with the CA Tape Encryption objects. The following is an example of the object tree displaying the CA Tape Encryption objects:



CA Tape Encryption Object List

CA Tape Encryption provides the following objects for viewing and analysis from the Windows Client:

Object	Description
Subsystem Address Space	Displays the active CA Tape Encryption Subsystem Address Spaces on the z/OS system that you have connected to.
Tape Encryption Details	Displays detailed information on the last 1000 encrypted or decrypted files for each active subsystem.
Statistics	Displays a month-by-month count of the number of tape file encryptions for the last 12 months.
Symmetric Keys	Displays the current key instance for each key defined to the active subsystems.
Key Rings	Displays all the key rings defined for all subsystems.
Display Activity	Displays the encryption and decryption jobs running on the z/OS system that you have connected to.
Display Status	Displays the status of important parameters and details about the cryptographic environment for each subsystem.
Encryption Selection	Displays data set encryption selection criteria from the SMS data class and the external security system.
B2BCodeBooks	Displays information about the code books defined in the B2BBOOKS parmlib member.
Security Definitions	Displays all security definitions that affect CA Tape Encryption.
Security Modes	Displays the security modes for each active CA Tape Encryption address space.

Standard Features in the Windows Client

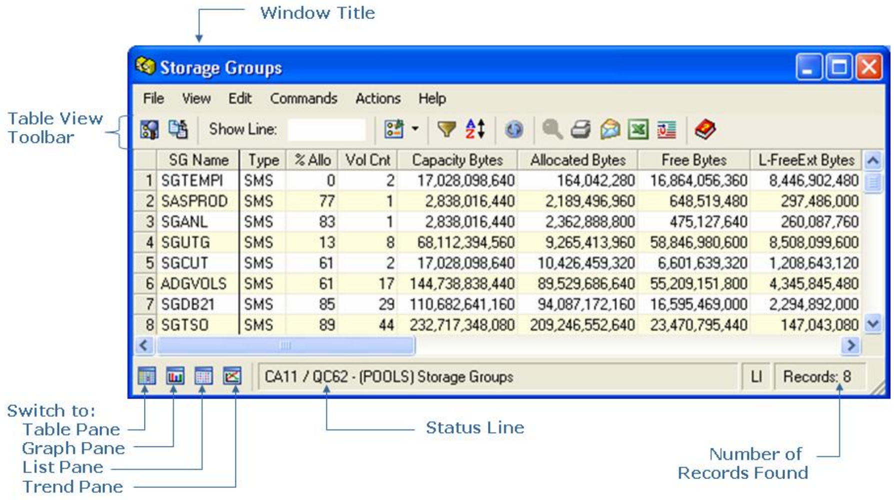
The following are examples of some of the standard features of the Windows Client.

Table Views

The default view for the Windows Client is Table View. The Table View displays objects in configurable tables. You can change display characteristics (such as the width and number of table columns, the number of rows displayed, and so on) and characteristics that apply to specific objects, such as sort and filter criteria. The display and object-specific characteristics determine the appearance of the table. When you save your user-defined views, you automatically save the display and object characteristics with it.

Note: To immediately view certain changes, like filters and sorts, you must click the Refresh icon .

The following is a sample of the Table View:

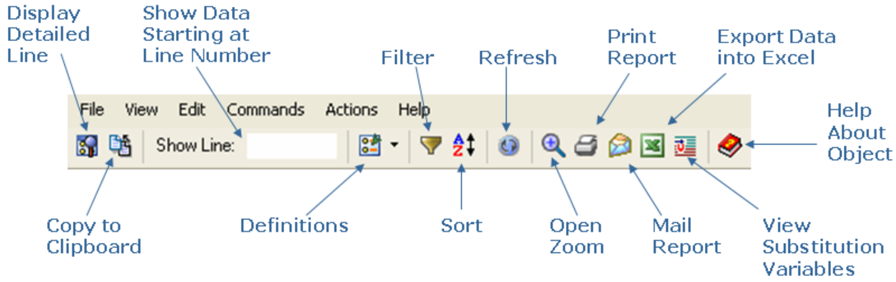


	SG Name	Type	% Allo	Vol Cnt	Capacity Bytes	Allocated Bytes	Free Bytes	L-FreeExt Bytes
1	SGTEMPI	SMS	0	2	17,028,098,640	164,042,280	16,864,056,360	8,446,902,480
2	SASPROD	SMS	77	1	2,838,016,440	2,189,496,960	648,519,480	297,486,000
3	SGANL	SMS	83	1	2,838,016,440	2,362,888,800	475,127,640	260,087,760
4	SGUTG	SMS	13	8	68,112,394,560	9,265,413,960	58,846,980,600	8,508,099,600
5	SGCUT	SMS	61	2	17,028,098,640	10,426,459,320	6,601,639,320	1,208,643,120
6	ADGVOLS	SMS	61	17	144,738,838,440	89,529,686,640	55,209,151,800	4,345,845,480
7	SGDB21	SMS	85	29	110,682,641,160	94,087,172,160	16,595,469,000	2,294,892,000
8	SGTSO	SMS	89	44	232,717,348,080	209,246,552,640	23,470,795,440	147,043,080

CA11 / QC62 - (POOLS) Storage Groups | LI | Records: 8

Table View Dialog Toolbar Options

The Table View dialog toolbar provides the following options:



Graph Views

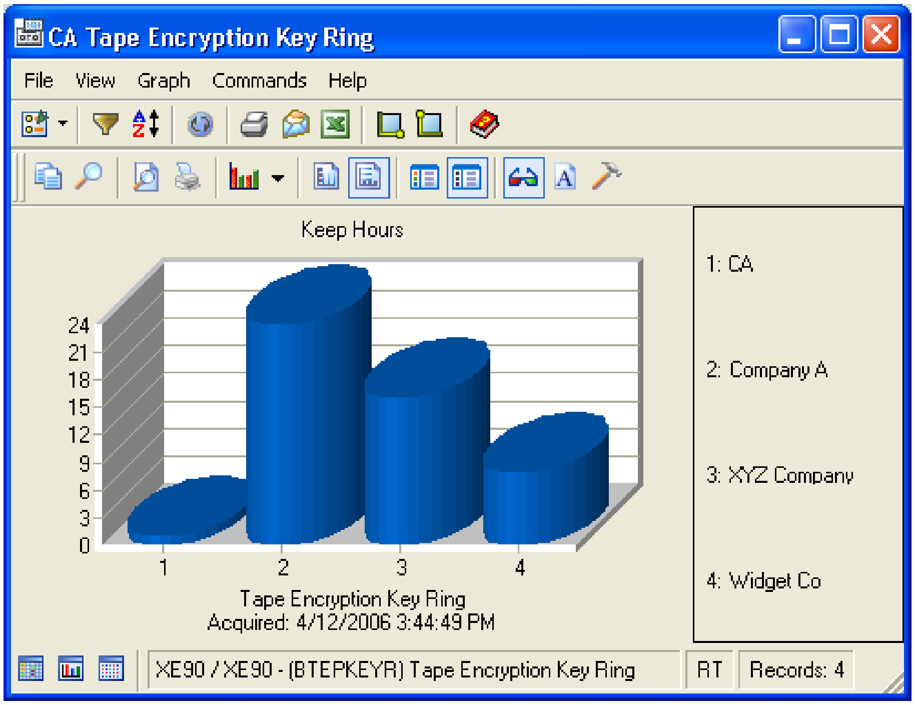
The Graph View feature displays a selected set of data in a graph. The Windows Client offers a large variation of graph types to present your data in a variety of formats. Some of the available graph types are:

- Line
- Point
- Area-curve
- Bar
- Pie
- Doughnut
- Pyramid
- Cube

You can specify the graph type and its format to obtain the kind of display you prefer. You can preview the general look of a graph while defining its various features.

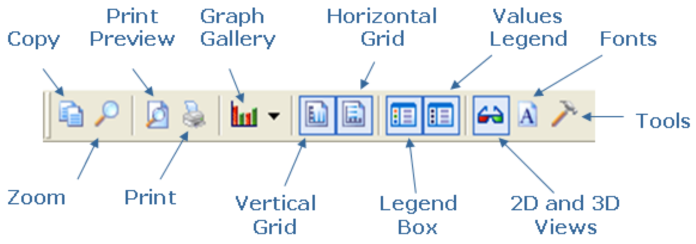
Note: To immediately view certain changes, you must click the Refresh icon .

The following sample graph shows the Keep Hours for four CA Tape Encryption key rings. The legend on the right side of the graph maps the numbers on the X-axis to the full content of what the axis represents. In this case, the X-axis represents the Alias Name for each ring. This setup allows you to identify the bars in the graph without cluttering the data.



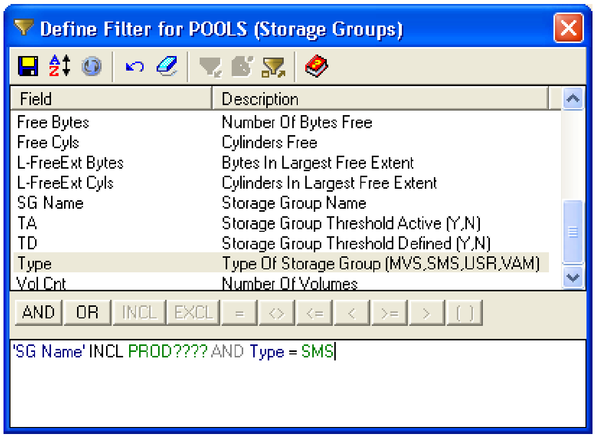
Graph View Dialog Toolbar Options

The Graph dialog toolbar provides you with these tools for working with graphs:



Filter

The Filter feature narrows the list of objects displayed in the table. The Windows Client lists the object fields in the Filter dialog in alphabetical order by field name. The Filter dialog guides you in the process of defining the filter expression by enabling and disabling the appropriate fields and controls at every step. The following is a sample of the Filter dialog:

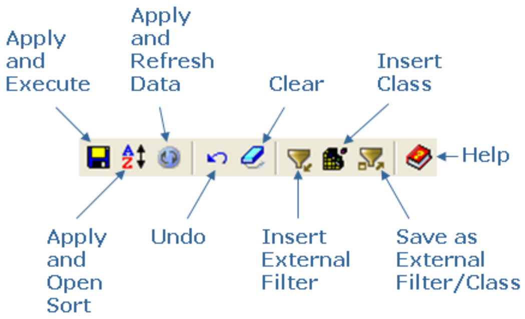


Field	Description
Free Bytes	Number Of Bytes Free
Free Cyls	Cylinders Free
L-FreeExt Bytes	Bytes In Largest Free Extent
L-FreeExt Cyls	Cylinders In Largest Free Extent
SG Name	Storage Group Name
TA	Storage Group Threshold Active (Y,N)
TD	Storage Group Threshold Defined (Y,N)
Type	Type Of Storage Group (MVS,SMS,USR,VAM)
Vol Cnt	Number Of Volumes

'SG Name' INCL PROD???? AND Type = SMS

Filter Dialog Toolbar Options

The Filter dialog toolbar provides the following options:



A filter can be built from the fields of the objects displayed in a window by combining them into Boolean expressions. You can also use expressions that contain patterns with wildcard characters.

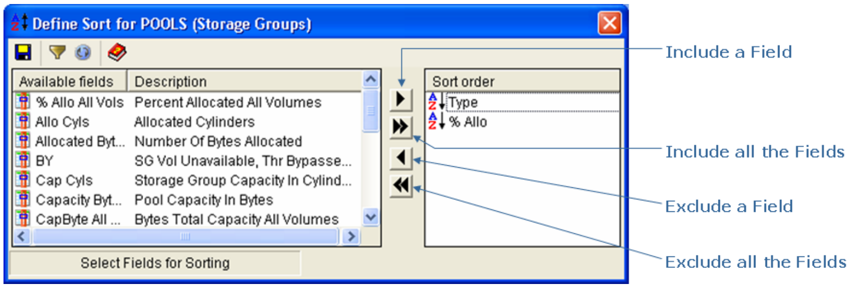
Refine your filter by using the AND/OR logical operators to combine several expressions is also possible. Use parentheses to group sub-expressions.

You can enter a filter expression directly into the text box at the bottom of the Define Filter dialog or use the typing aids in the dialog. It is possible to edit any expression in the text box.

Note: To immediately view the effect of your filter you must click the Apply and Refresh Data icon .

Sort

The Sort feature sorts the table by the values in the columns of the table. Every object attribute (or field for z/OS) in a table can serve as a sort key, as shown in the following sample:



Define Sort for POOLS (Storage Groups)

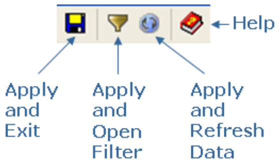
Available fields	Description
% Allo All Vols	Percent Allocated All Volumes
Allo Cyls	Allocated Cylinders
Allocated Byt...	Number Of Bytes Allocated
BY	SG Vol Unavailable, Thr Bypasse...
Cap Cyls	Storage Group Capacity In Cylind...
Capacity Byt...	Pool Capacity In Bytes
CapByte All ...	Bytes Total Capacity All Volumes

Sort order
Type
% Allo

Note: To immediately view the effect of your sort you must click the Apply and Refresh Data icon .

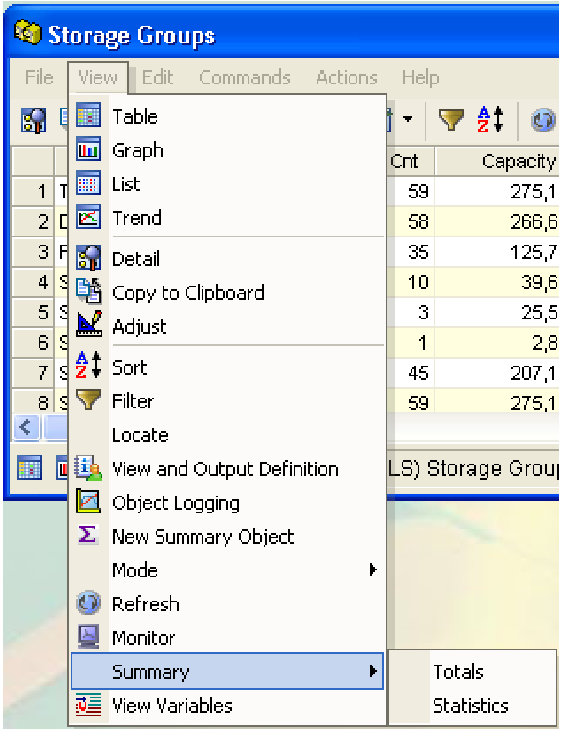
Sort Dialog Toolbar Options

The Sort dialog toolbar provides the following options:



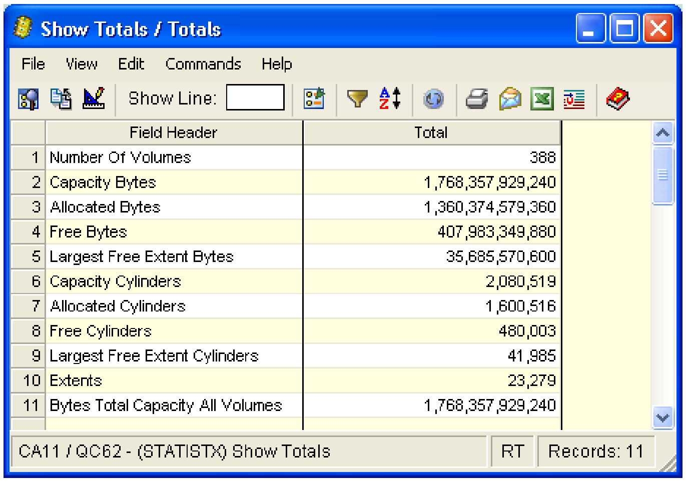
Summary Totals and Statistics (average, min and max)

The View menu for every table lets you request the total of every numeric field, or to combine the totals with the average, min and max values as well. The following example shows how to access Summary Totals and Statistics:



Totals

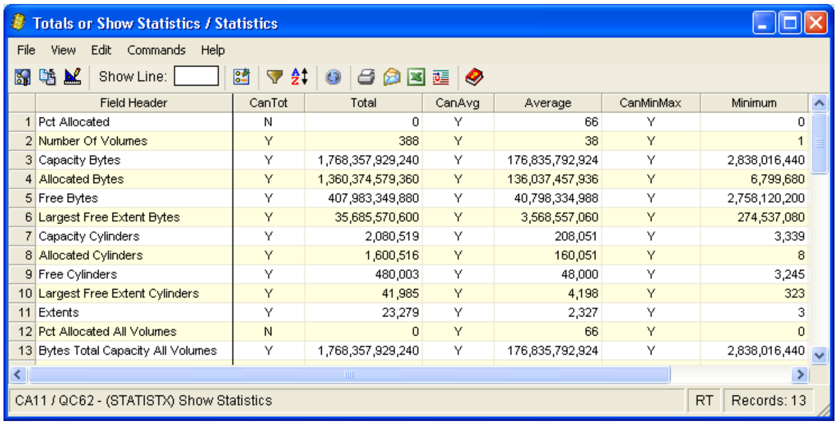
The Totals option provides a sum of all numeric fields, as shown in the following example:



	Field Header	Total
1	Number Of Volumes	388
2	Capacity Bytes	1,768,357,929,240
3	Allocated Bytes	1,360,374,579,360
4	Free Bytes	407,983,349,880
5	Largest Free Extent Bytes	35,685,570,600
6	Capacity Cylinders	2,080,519
7	Allocated Cylinders	1,600,516
8	Free Cylinders	480,003
9	Largest Free Extent Cylinders	41,985
10	Extents	23,279
11	Bytes Total Capacity All Volumes	1,768,357,929,240

CA11 / QC62 - (STATISTX) Show Totals | RT | Records: 11

The Statistics option provides totals plus the average min and max values for all numeric fields, as shown in the following example:


Totals or Show Statistics / Statistics
File View Edit Commands Help
Show Line:

	Field Header	CanTot	Total	CanAvg	Average	CanMinMax	Minimum
1	Pct Allocated	N	0	Y	66	Y	0
2	Number Of Volumes	Y	388	Y	38	Y	1
3	Capacity Bytes	Y	1,768,357,929,240	Y	176,835,792,924	Y	2,838,016,440
4	Allocated Bytes	Y	1,360,374,579,360	Y	136,037,457,936	Y	6,799,680
5	Free Bytes	Y	407,983,349,880	Y	40,798,334,988	Y	2,758,120,200
6	Largest Free Extent Bytes	Y	35,685,570,600	Y	3,568,557,060	Y	274,537,080
7	Capacity Cylinders	Y	2,080,519	Y	208,051	Y	3,339
8	Allocated Cylinders	Y	1,600,516	Y	160,051	Y	8
9	Free Cylinders	Y	480,003	Y	48,000	Y	3,245
10	Largest Free Extent Cylinders	Y	41,985	Y	4,198	Y	323
11	Extents	Y	23,279	Y	2,327	Y	3
12	Pct Allocated All Volumes	N	0	Y	66	Y	0
13	Bytes Total Capacity All Volumes	Y	1,768,357,929,240	Y	176,835,792,924	Y	2,838,016,440

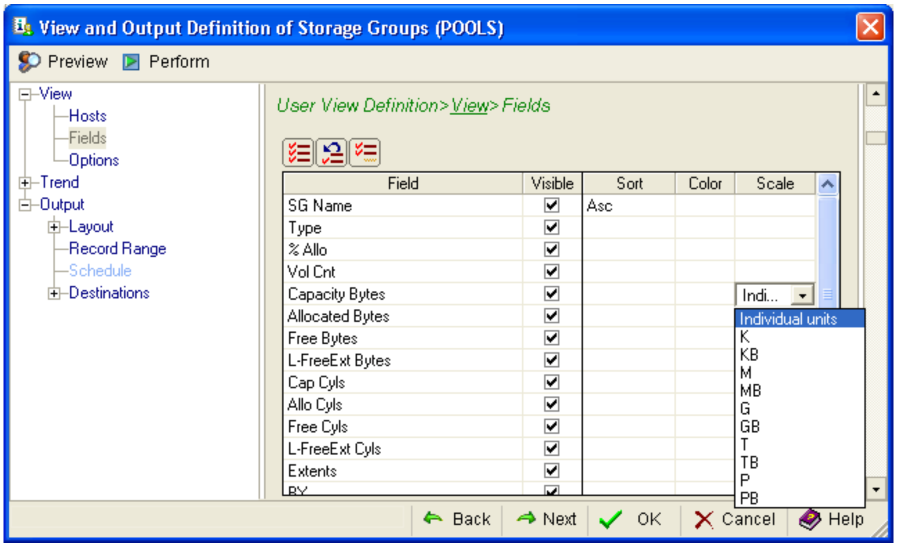
CA11 / QC62 - (STATISTX) Show Statistics | RT | Records: 13

Scaling

The Scale option list lets you select the scale base units for displaying numerical data. The difference between requesting K, M, G, and so on, versus KB, MB, GB and so on is that those with the appended B mean multiples of 1024, while those without the B mean multiples of 1000. For example:

- *nn*K = *nn*(1000), *nn*M = *nn*(1000)(1000), and so on.
- *nn*KB = *nn*(1024), *nn*MB = *nn*(1024)(1024), and so on.

The following is a sample of the change Field Scale dialog:

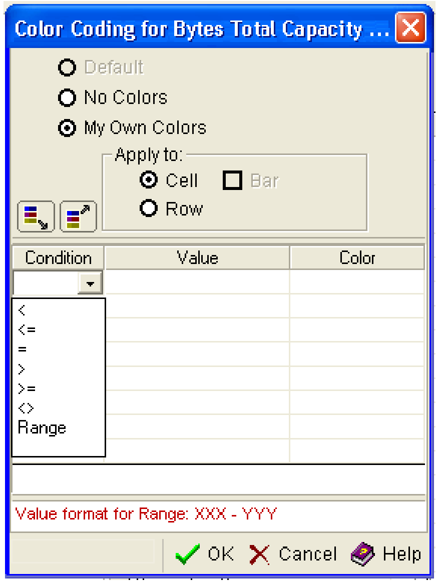


Field	Visible	Sort	Color	Scale
SG Name	☑	Asc		
Type	☑			
% Allo	☑			
Vol Cnt	☑			
Capacity Bytes	☑			Indi...
Allocated Bytes	☑			
Free Bytes	☑			
L-FreeExt Bytes	☑			
Cap Cyls	☑			
Allo Cyls	☑			
Free Cyls	☑			
L-FreeExt Cyls	☑			
Extents	☑			
BY	☑			

Individual units
K
KB
M
MB
G
GB
T
TB
P
PB

Color Coding

You can set conditions for color coding values in object views. The following sample shows you can select a Condition, enter a condition Value, and then select a Color which will show as the background color in the object view for the item that meets the condition:



Color Coding for Bytes Total Capacity ...

○ Default

○ No Colors

● My Own Colors

Apply to:

● Cell □ Bar

○ Row

Condition	Value	Color

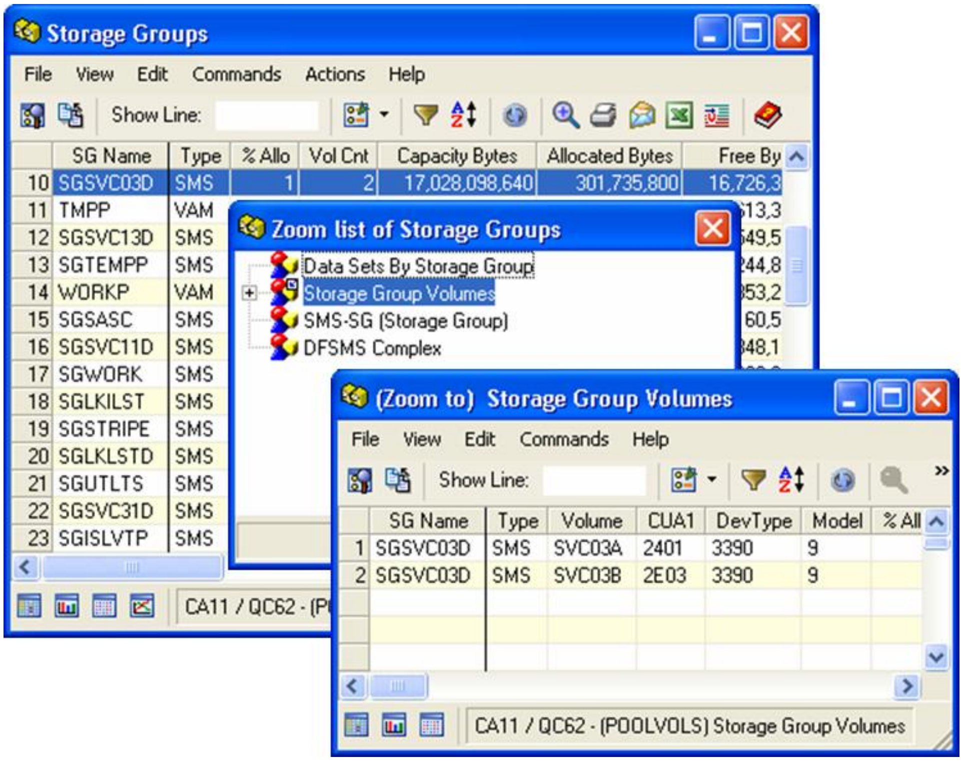
<
<=
=
>
>=
<>
Range

Value format for Range: XXX - YYY

Open Zoom (Drill-Down Feature)

The Open Zoom feature provides you with a list of objects that have related information. You can select an object from the Zoom list dialog to view the related information.

The following example illustrates a zoom from the Storage Groups object to the Storage Group Volumes object:



	SG Name	Type	% Allo	Vol Cnt	Capacity Bytes	Allocated Bytes	Free By
10	SGSVC03D	SMS	1	2	17,028,098,640	301,735,800	16,726,3
11	TMPP	VAM					13,3
12	SGSVC13D	SMS					49,5
13	SGTEMPP	SMS					44,8
14	WORKP	VAM					53,2
15	SGSASC	SMS					60,5
16	SGSVC11D	SMS					48,1
17	SGWORK	SMS					
18	SGLKILST	SMS					
19	SGSTRIPE	SMS					
20	SGLKLSTD	SMS					
21	SGUTLTS	SMS					
22	SGSVC31D	SMS					
23	SGISLVTP	SMS					

CA11 / QC62 - (P

- Data Sets By Storage Group
- Storage Group Volumes
- SMS-SG (Storage Group)
- DFSMS Complex

	SG Name	Type	Volume	CUA1	DevType	Model	% All
1	SGSVC03D	SMS	SVC03A	2401	3390	9	
2	SGSVC03D	SMS	SVC03B	2E03	3390	9	

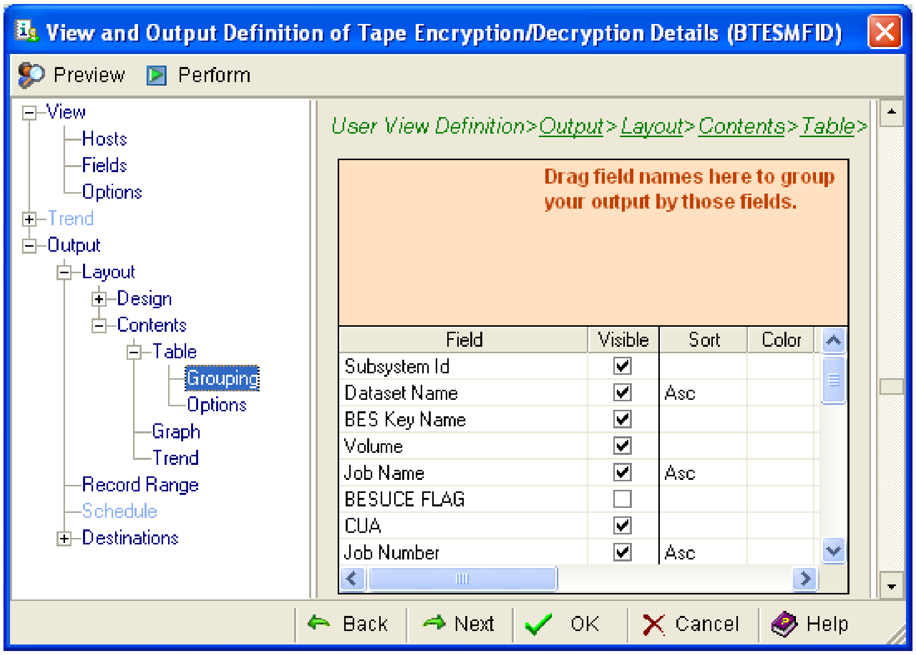
CA11 / QC62 - (POOLVOLS) Storage Group Volumes

Customized Reports

You can customize reports with the appearance and information you want by clicking the Definitions icon from the toolbar of the object view.

For example, in CA Tape Encryption, you could create a report based on the Tape Encryption/Decryption Details view that contained information on the Subsystem ID, BES Key Name, Volume, and other fields. You could then sort the report by Dataset Name, Job Name, and then Job Number, in that order.

The following example shows how you would define this report in the Output and View Definition wizard.



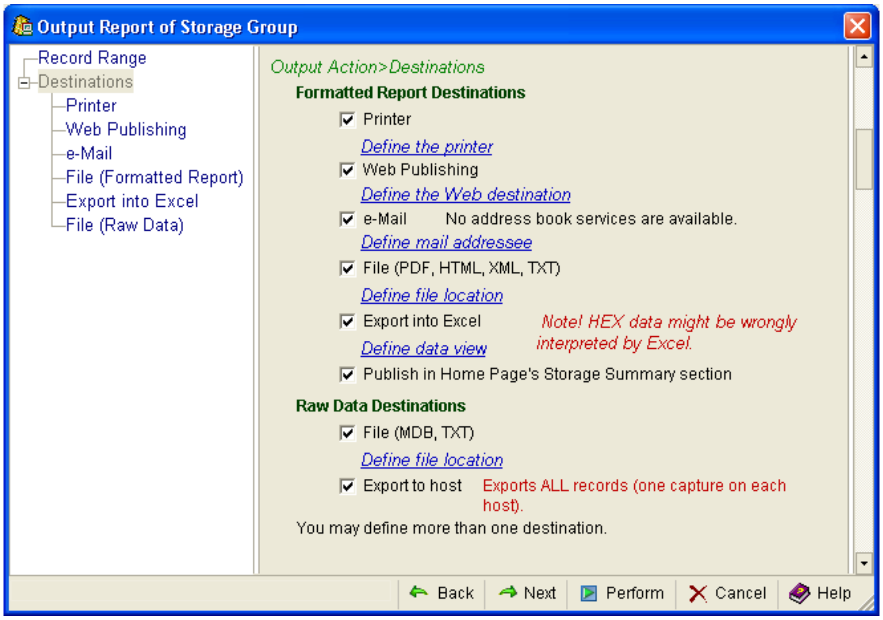
User View Definition>Output>Layout>Contents>Table>

Drag field names here to group your output by those fields.

Field	Visible	Sort	Color
Subsystem Id	☑		
Dataset Name	☑	Asc	
BES Key Name	☑		
Volume	☑		
Job Name	☑	Asc	
BESUCE FLAG	☐		
CUA	☑		
Job Number	☑	Asc	

Multiple Output Formats

When you select Destinations in the Output Action dialog you can indicate where you want a report to be published, as shown in the following sample:



Output Report of Storage Group

Output Action>Destinations

Formatted Report Destinations

☑ Printer
Define the printer

☑ Web Publishing
Define the Web destination

☑ e-Mail No address book services are available.
Define mail addressee

☑ File (PDF, HTML, XML, TXT)
Define file location

☑ Export into Excel *Note! HEX data might be wrongly interpreted by Excel.*
Define data view

☑ Publish in Home Page's Storage Summary section

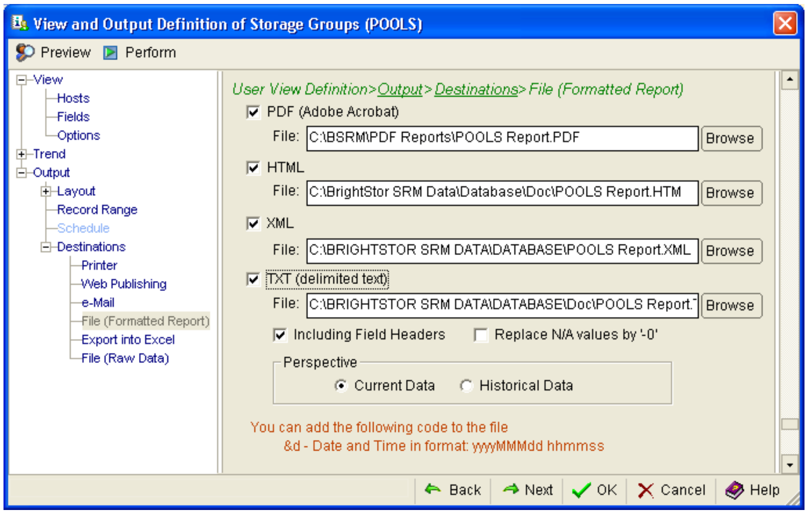
Raw Data Destinations

☑ File (MDB, TXT)
Define file location

☑ Export to host Exports ALL records (one capture on each host).

You may define more than one destination.

Each Output Destination gives you additional options; for example, the File (Formatted Report) destination dialog gives you the choice of file formats and a Browse button that allows you to select the output directory, as shown in the following sample:



View and Output Definition of Storage Groups (POOLS)

User View Definition>Output>Destinations>File (Formatted Report)

☑ PDF (Adobe Acrobat)
File: C:\BSRM\PDF Reports\POOLS Report.PDF Browse

☑ HTML
File: C:\BrightStor SRM Data\Database\Doc\POOLS Report.HTM Browse

☑ XML
File: C:\BRIGHTSTOR SRM DATA\DATABASE\POOLS Report.XML Browse

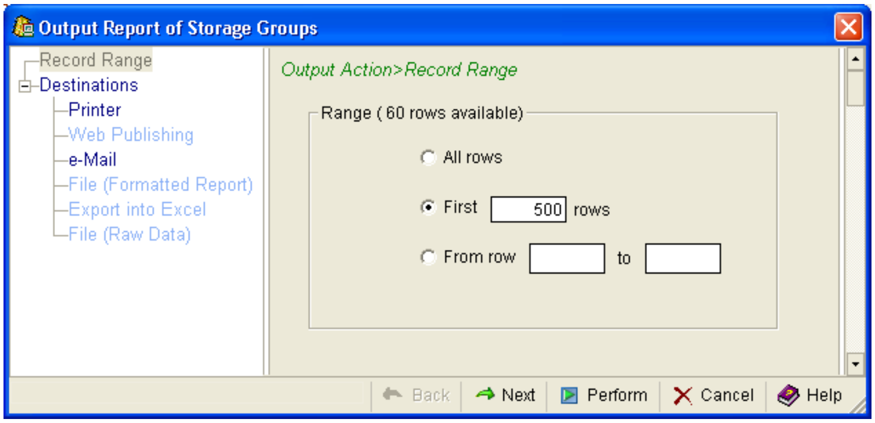
☑ TXT (delimited text)
File: C:\BRIGHTSTOR SRM DATA\DATABASE\Doc\POOLS Report.T Browse

☑ Including Field Headers ☐ Replace N/A values by '-0'

Perspective
● Current Data ○ Historical Data

You can add the following code to the file
&d - Date and Time in format: yyyyMMdd hhmmss

If you want to quickly print or send the information shown in the view to multiple destinations, click the Print Report icon or the Mail Report icon from the toolbar of the object view. This will give you the following Output Action dialog:



Output Action>Record Range

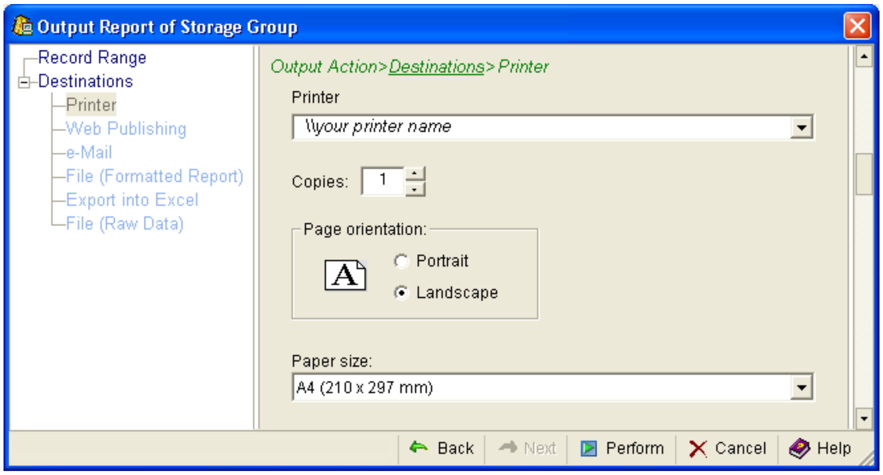
Range (60 rows available)

○ All rows

● First 500 rows

○ From row to

If you selected the Print Report icon , you will also be provided with the Printer destination dialog, as shown in the following sample:



Output Action>Destinations>Printer

Printer: \\your printer name

Copies: 1

Page orientation:

○ Portrait

● Landscape

Paper size: A4 (210 x 297 mm)

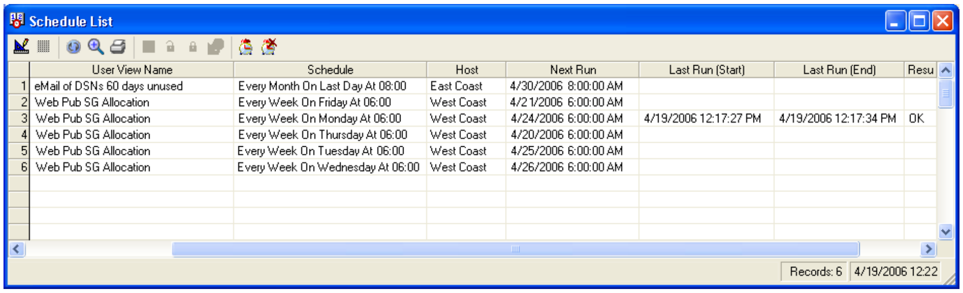
See the *CA Vantage Windows Client User Guide* for more information about Output Definitions.

Schedulers

The Scheduler provides a consistent set of scheduling services for all output activities within the Windows Client environment, for both on-demand and automated events. You can schedule events by day, hour, and minute, or as a delay specified in years, days, hours, and minutes.

For instance, suppose you wanted to be kept relatively up-to-date on the status of currently active encryption and decryption activity. To do this, you could schedule a report based on the Tape Encryption/Decryption Details display to run every morning at 9:00 AM. Set the Destination of the report to Web Publishing. With this setup, GMI would automatically run a report on current encryption and decryption activity every morning and publish the report to the web.

The Windows Client also includes a Schedule List. This is a list of all your scheduled activities. You can use the Schedule List option to start the scheduler and manage scheduled items. The following is an example of the Schedule List dialog:

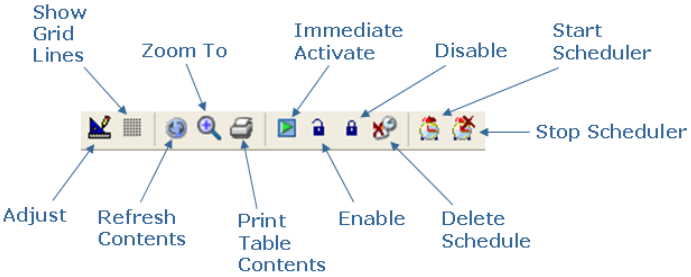


	User View Name	Schedule	Host	Next Run	Last Run (Start)	Last Run (End)	Resu
1	eMail of DSNs 60 days unused	Every Month On Last Day At 08:00	East Coast	4/30/2006 8:00:00 AM			
2	Web Pub SG Allocation	Every Week On Friday At 06:00	West Coast	4/21/2006 6:00:00 AM			
3	Web Pub SG Allocation	Every Week On Monday At 06:00	West Coast	4/24/2006 6:00:00 AM	4/19/2006 12:17:27 PM	4/19/2006 12:17:34 PM	OK
4	Web Pub SG Allocation	Every Week On Thursday At 06:00	West Coast	4/20/2006 6:00:00 AM			
5	Web Pub SG Allocation	Every Week On Tuesday At 06:00	West Coast	4/25/2006 6:00:00 AM			
6	Web Pub SG Allocation	Every Week On Wednesday At 06:00	West Coast	4/26/2006 6:00:00 AM			

Records: 6 4/19/2006 12:22

Schedule List Dialog Toolbar Options

The Schedule List dialog provides the following toolbar options:



Note: For more information about the Scheduler and Schedule List, see the *CA Vantage* Windows *Client User Guide*.

JCL Management

CA GMI supports two methods of job submission:

- Manual
- Automatic

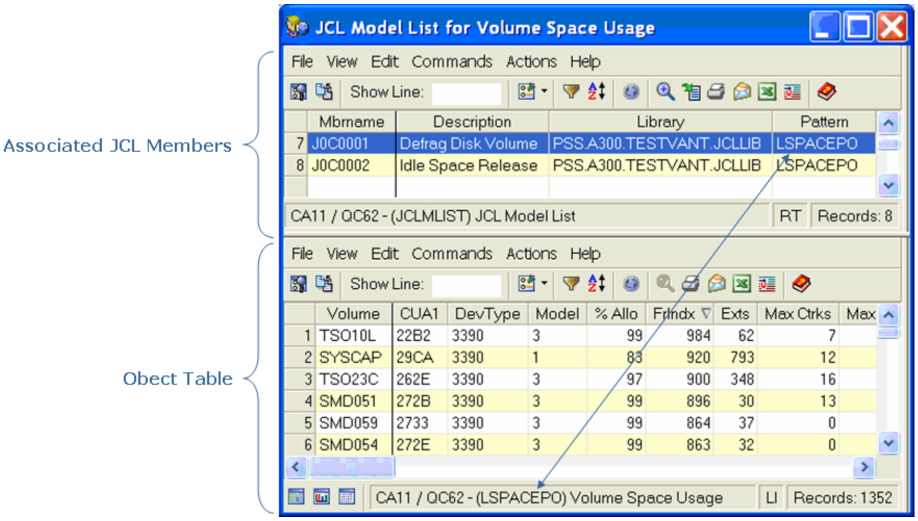
You can submit jobs manually from the Windows Client, either immediately or at a scheduled time. When you create a job (JCL stream) to submit, you determine the type of job being submitted, the number of steps, and so on. The job can involve CA Tape Encryption, standard IBM utility programs, your own utility programs, or any combination of these. You can also use IEFBR14 jobs for testing purposes.

CA GMI helps you specify substitution variables (symbolic parameters) in the sample JCL you provide, allowing you to create generalized model JCL. Whenever CA GMI submits a job to the internal reader, it first scans the entire JCL stream, finds all the variable names, and substitutes the current values for all the variables that were used.

The Windows Client also has an Edit Member (and Submit) function under the z/OS menu in the Main Window. You can use the Drag and Drop feature to drag rows from object displays and drop them onto a JCL template in the Edit dialog. Substitution from the rows into the Variables in the template will be done.

CA GMI also has a feature for helping you manage JCL, the JCL Model List feature. You can use this feature to select JCL models to be used by objects or a group of objects using pattern matching. These models can be used to perform actions or storage management functions in batch jobs. The models can contain object variables that will be substituted upon request or at submit time.

The following is an example of what you see when you select JCL Model List. The dialog that appears contains both the object table and the list of associated JCL members.


Associated JCL Members
Obect Table
JCL Model List for Volume Space Usage
File View Edit Commands Actions Help
Show Line:
File View Edit Commands Actions Help
Show Line:

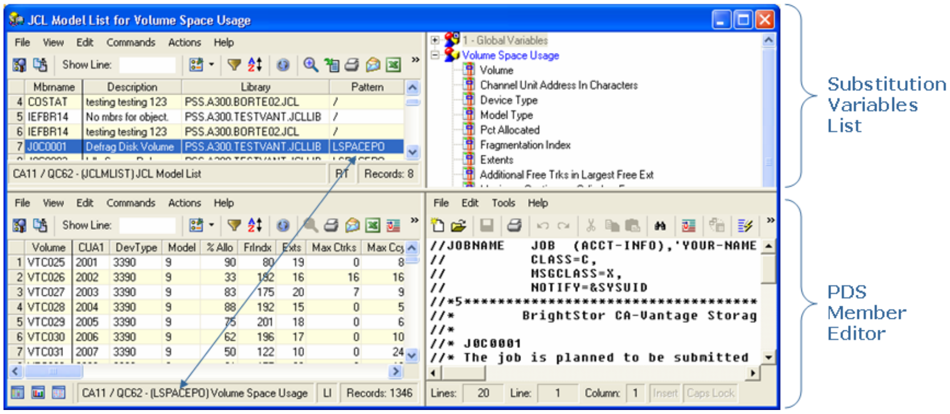
	Mbrname	Description	Library	Pattern
7	J0C0001	Defrag Disk Volume	PSS.A300.TESTVANT.JCLLIB	LSPACEPO
8	J0C0002	Idle Space Release	PSS.A300.TESTVANT.JCLLIB	LSPACEPO

CA11 / QC62 - (JCLMLIST) JCL Model List | RT | Records: 8

	Volume	CUA1	DevType	Model	% Allo	FrIndx ▽	Exts	Max Ctrks	Max
1	TSO10L	22B2	3390	3	99	984	62	7	
2	SYSCAP	29CA	3390	1	83	920	793	12	
3	TSO23C	262E	3390	3	97	900	348	16	
4	SMD051	272B	3390	3	99	896	30	13	
5	SMD059	2733	3390	3	99	864	37	0	
6	SMD054	272E	3390	3	99	863	32	0	

CA11 / QC62 - (LSPACEPO) Volume Space Usage | LI | Records: 1352

You can double-click a model line, and the “Substitution Variable List” for the object and the “PDS Member Editor” will open up with the JCL. You can then add variables by double-clicking them from the “Substitution Variables List” pane and then dragging selected lines from the source object to the “PDS Member Editor” pane. The JCL member created can then be substituted and submitted.


JCL Model List for Volume Space Usage
File View Edit Commands Actions Help
Show Line:
CA11 / QC62 - (JCLMLIST) JCL Model List
RT
Records: 8
1 - Global Variables
Volume Space Usage
Volume
Channel Unit Address In Characters
Device Type
Model Type
Pct Allocated
Fragmentation Index
Extents
Additional Free Trks in Largest Free Ext
File View Edit Commands Actions Help
Show Line:
CA11 / QC62 - (LSPACEPO) Volume Space Usage
LI
Records: 1346
File Edit Tools Help
Lines: 20 Line: 1 Column: 1 Insert Caps Lock
Substitution Variables List
PDS Member Editor

	Mbrname	Description	Library	Pattern
4	COSTAT	testing testing 123	PSS.A300.BORTE02.JCL	/
5	IEFBR14	No mbrs for object.	PSS.A300.TESTVANT.JCLLIB	/
6	IEFBR14	testing testing 123	PSS.A300.BORTE02.JCL	/
7	J0C0001	Defrag Disk Volume	PSS.A300.TESTVANT.JCLLIB	LSPACEPO

	Volume	CUA1	DevType	Model	% Allo	Frlndx	Exts	Max Ctrks	Max Ccy
1	VTC025	2001	3390	9	90	80	19	0	8
2	VTC026	2002	3390	9	33	182	16	16	16
3	VTC027	2003	3390	9	83	175	20	7	9
4	VTC028	2004	3390	9	88	192	15	0	5
5	VTC029	2005	3390	9	75	201	18	0	6
6	VTC030	2006	3390	9	62	196	17	0	10
7	VTC031	2007	3390	9	50	122	10	0	24

```
//JOBNAME    JOB  (ACCT-INFO),'YOUR-NAME
//             CLASS=C,
//             MSGCLASS=X,
//             NOTIFY=&SYSUID
//*5************************************
//*          BrightStor CA-Vantage Storag
//*
//* J0C0001
//* The job is planned to be submitted
```

From the “PDS Member Editor” pane you can also manipulate and save the JCL member.

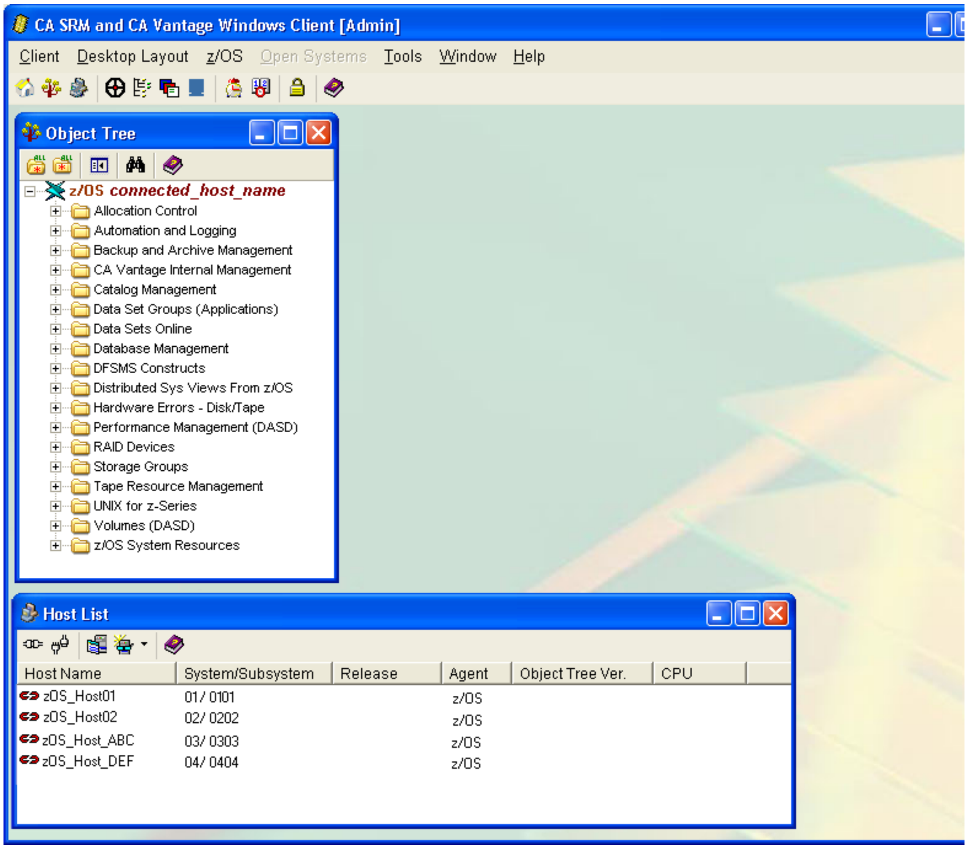
Chapter 2: Auditing CA Tape Encryption

This section contains the following topics:

Start the Windows Client

You can open the Windows Client from the Start menu by clicking Start, Programs, CA, CA Storage Resource Manager, Windows Client.

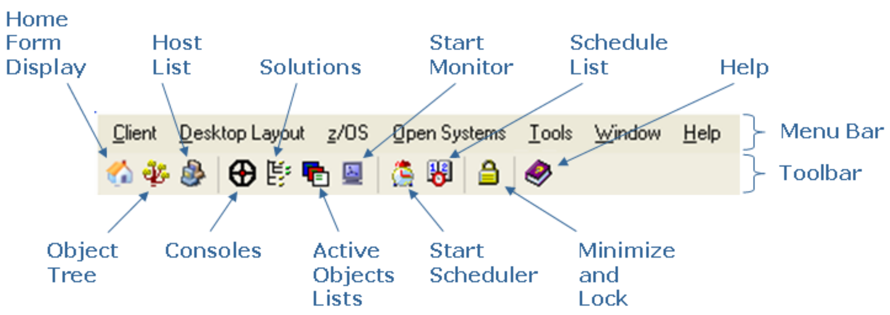
The following sample of the Windows Client displays the z/OS Object Tree and the Host List dialogs. You can decide which dialogs to display and where to put them in the Main Window.



Host Name	System/Subsystem	Release	Agent	Object Tree Ver.	CPU
zOS_Host01	01/ 0101		z/OS		
zOS_Host02	02/ 0202		z/OS		
zOS_Host_ABC	03/ 0303		z/OS		
zOS_Host_DEF	04/ 0404		z/OS		

Windows Client Menu Bar and Toolbar Options

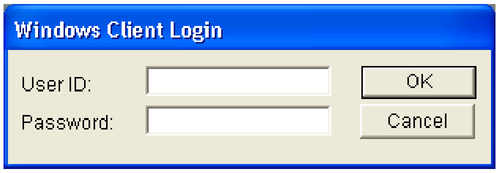
The top of the Main Window of the Windows Client has the following menu bar and toolbar, as shown in the following sample:



Note: The Windows Client menu bar and toolbar options are explained in the *CA Vantage Client User Guide*.

Log in to the Windows Client

By default, when you start the Windows Client, you automatically log in as the ADMIN user (the default administrator) and no Login dialog appears. However, if this default was changed to require a specific user ID and password, the following Login dialog appears, as shown in the following sample:



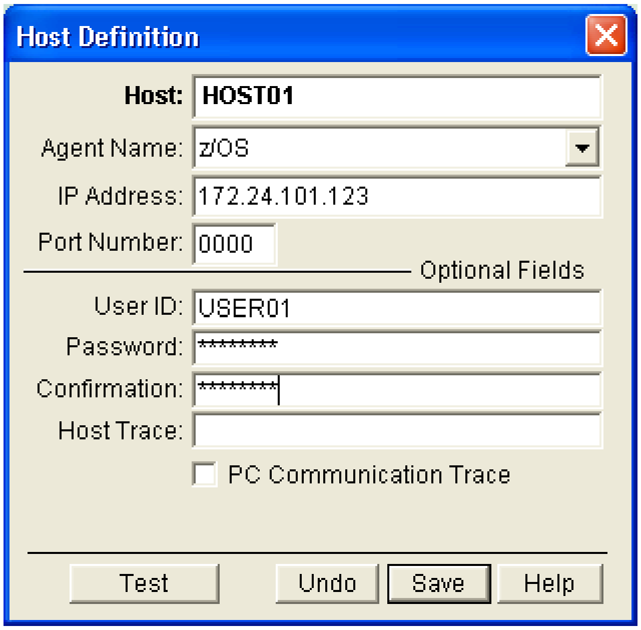
Define the z/OS Host

After logging in to the Windows Client, you need to define the z/OS servers that you plan to use.

To define a z/OS host

1. From the Host Definition dialog, click the New Host or View Host Definition icon.

   The Host Definition dialog opens, as shown in the following sample:



Host Definition

Host: HOST01

Agent Name: z/OS

IP Address: 172.24.101.123

Port Number: 0000

Optional Fields

User ID: USER01

Password: ********

Confirmation: ********

Host Trace:

□ PC Communication Trace

2. Complete the dialog, noting the following:

   - **IP Address and Port Number:** When you select a z/OS host, you must supply both an IP address and a port number. You can verify that the values are valid by clicking the Test button at the bottom of the dialog. The Windows Client displays a message indicating whether the connectivity test succeeded or failed.

   - **User ID and Password:** The User ID and Password are optional. If you do not specify values for these fields, then you must enter a User ID and Password every time you log into the Windows Client.

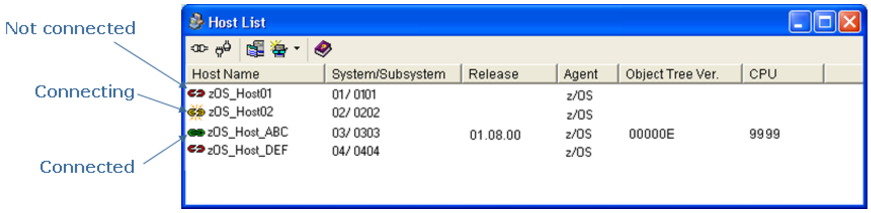
   - **Undo and Save:** After you enter data in any field on the dialog, you must click Save or Undo.

3. Click Test to test your connection information.

   The Windows Client will advise you if your connection is successful.

4. Click Save.

   The Windows Client stores the host definition. The definition will be displayed in the Host List dialog. The Host List dialog displays defined hosts and their connection status, as shown in the following sample:

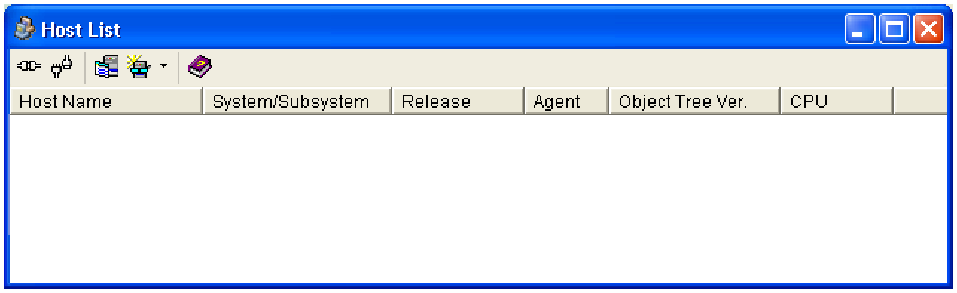


Host Name	System/Subsystem	Release	Agent	Object Tree Ver.	CPU
zOS_Host01	01/ 0101		z/OS		
zOS_Host02	02/ 0202		z/OS		
zOS_Host_ABC	03/ 0303	01.08.00	z/OS	00000E	9999
zOS_Host_DEF	04/ 0404		z/OS		

Log in to the z/OS Host

After you log in to the Windows Client you must connect and log in to a z/OS host.

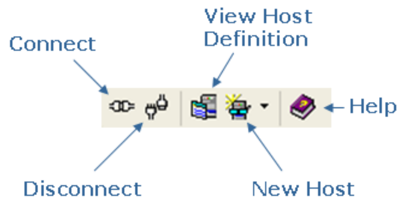
You connect and log in to a z/OS host from the Host List dialog. To display the Host List dialog click the Host List icon in the toolbar at the top of the Main Window of the Windows Client. If no hosts have been defined, then the Host List dialog will be empty, as shown in the following sample:



Host Name	System/Subsystem	Release	Agent	Object Tree Ver.	CPU

Host List Dialog Toolbar Options

The Host List dialog provides the following toolbar options:



To log in to a z/OS host

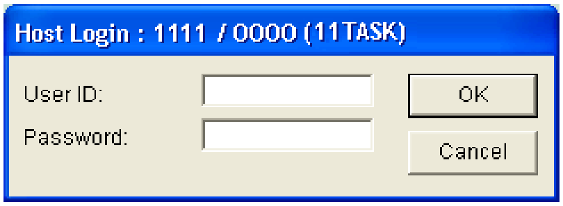
1. Select the host to which you want to log in from the Host List dialog.

   The selected row is highlighted.

2. Click the Connect icon .

   The connection status icon changes from the Not Connected icon , to the Connecting icon .

   If the user ID and password were not provided in the Host Definition, then the Host Login dialog is displayed, as shown in the following sample, and you must enter a valid user ID and password:

3. Click OK.

   When the log in is complete, the connection icon in the Host List Dialog changes from the Connecting icon , to the Connected icon .

Note: For more information about defining hosts and connecting to hosts, see the *CA Vantage Windows Client User Guide*.

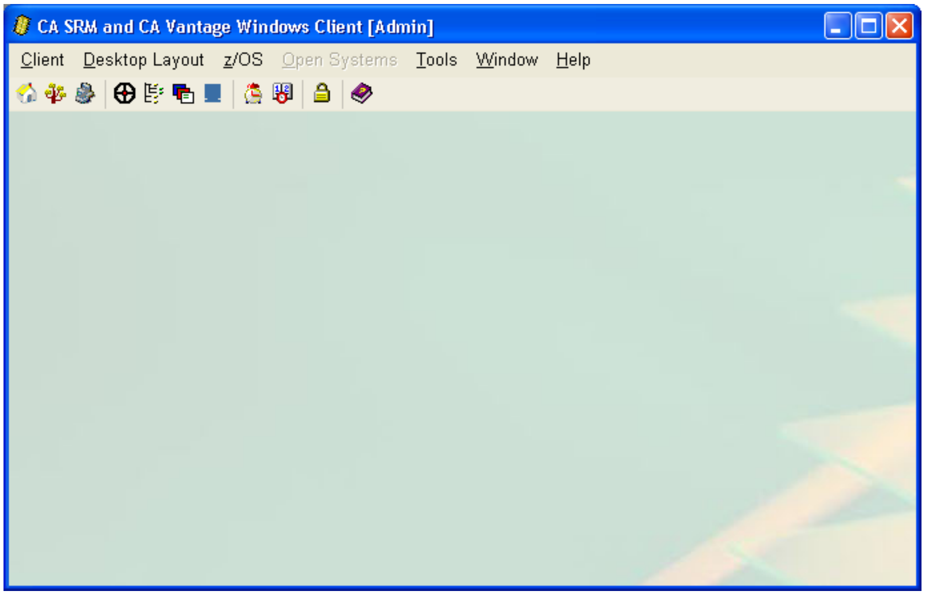
Access CA Tape Encryption Objects from the Windows Client

All CA Tape Encryption objects are included in the Windows Client Object Tree. They are contained within the Tape Resource Management folder that is visible when the Object Tree is opened.

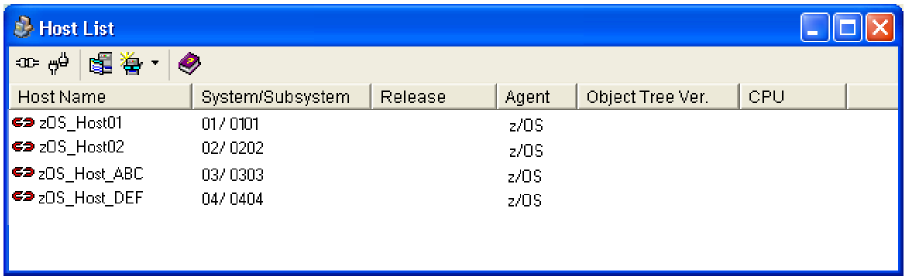
Before you begin, make sure that the z/OS host that you want to connect to is up-and-running.

To access CA Tape Encryption objects

1. Open the Windows Client from the Start Menu by clicking Programs, CA, CA Resource Manager, and then selecting Windows Client.
2. The Windows Client opens, as shown in the following sample:



3. From the toolbar, click the Host List icon .
4. The Host List dialog opens, as shown in the following sample:



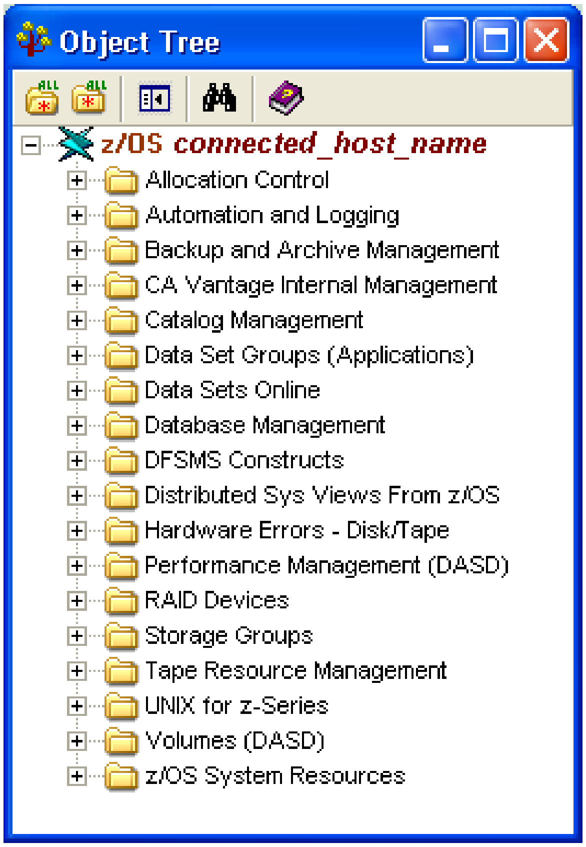
Host Name	System/Subsystem	Release	Agent	Object Tree Ver.	CPU
zOS_Host01	01/ 0101		z/OS		
zOS_Host02	02/ 0202		z/OS		
zOS_Host_ABC	03/ 0303		z/OS		
zOS_Host_DEF	04/ 0404		z/OS		

5. Select the z/OS host that you want to connect to and click the Connect icon .

6. CA GMI collects information from the z/OS host definition that you have chosen to connect to. Depending on how you have set up the Host Definition selected you may need to log on as described in the procedure To log in to a z/OS host, once you are connected to the host continue to step 4.

7. From the Windows Client Admin window, click the Object Tree icon to open the Object Tree.

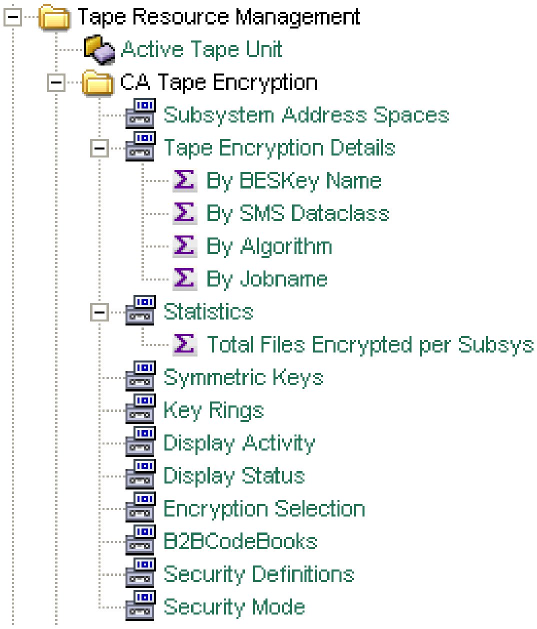
   The Object Tree dialog opens, as shown in the following sample:



Object Tree

z/OS connected_host_name
- Allocation Control
- Automation and Logging
- Backup and Archive Management
- CA Vantage Internal Management
- Catalog Management
- Data Set Groups (Applications)
- Data Sets Online
- Database Management
- DFSMS Constructs
- Distributed Sys Views From z/OS
- Hardware Errors - Disk/Tape
- Performance Management (DASD)
- RAID Devices
- Storage Groups
- Tape Resource Management
- UNIX for z-Series
- Volumes (DASD)
- z/OS System Resources

8. Expand the Tape Resource Management folder to display the CA Tape Encryption folder and, in turn, expand it to display the CA Tape Encryption objects, as shown in the following sample:



- Tape Resource Management
  - Active Tape Unit
  - CA Tape Encryption
    - Subsystem Address Spaces
    - Tape Encryption Details
      - By BESKey Name
      - By SMS Dataclass
      - By Algorithm
      - By Jobname
    - Statistics
      - Total Files Encrypted per Subsys
    - Symmetric Keys
    - Key Rings
    - Display Activity
    - Display Status
    - Encryption Selection
    - B2BCodeBooks
    - Security Definitions
    - Security Mode

For descriptions of the CA Tape Encryption objects, see the *CA Tape Encryption Object List* section in the chapter, “Introducing CA Tape Encryption.”

CA Tape Encryption Data Sources

When you open an object displayed in the object tree, the Windows Client displays data from all the active subsystems on the Logical Partition (LPAR) where CA Tape Encryption is installed.

Note that the CA Tape Encryption objects are *read-only*. They are defined and maintained using:

- The ISPF editor to define parmlib members. Data entered in parmlib is maintained in the CA Tape Encryption database.
- ISPF ISMF panels to update DFSMS data classes and other DFSMS resources.

The CA Tape Encryption data displayed in the Windows Client comes primarily from three sources:

- The CA Tape Encryption BES database (Symmetric Keys, Key Rings, Statistics, Display Status, B2BCodeBooks and Tape Encryption Details objects)
- The DFSMS control data set (CDS) active on the z/OS system where CA Tape Encryption is running (the Dataclass object)
- z/OS control blocks on the system where CA Tape Encryption is running (Subsystem Address Spaces, Display Status, Display Activity objects.) This includes information on ICSF and the tape management system routines found on the system.

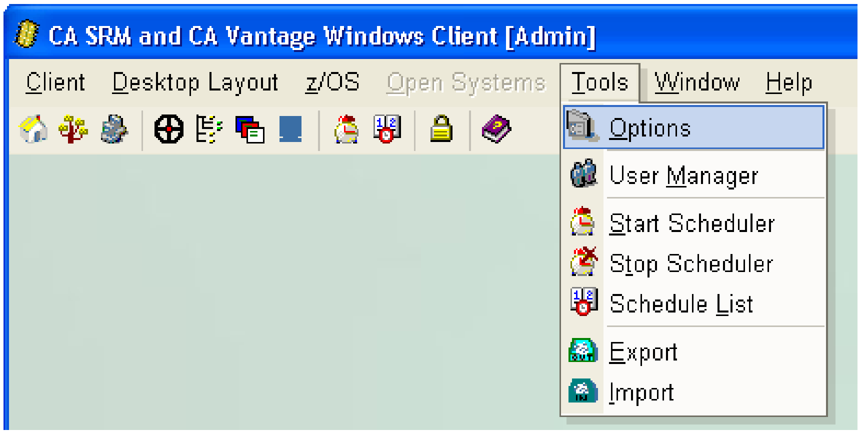
Data Collection Modes

CA GMI can be configured to collect data in either Automatic or Manual mode.

- In Automatic mode, data is collected when you open an object.
- In Manual mode, data is collected when you open an object and click the Execute icon ⚙.

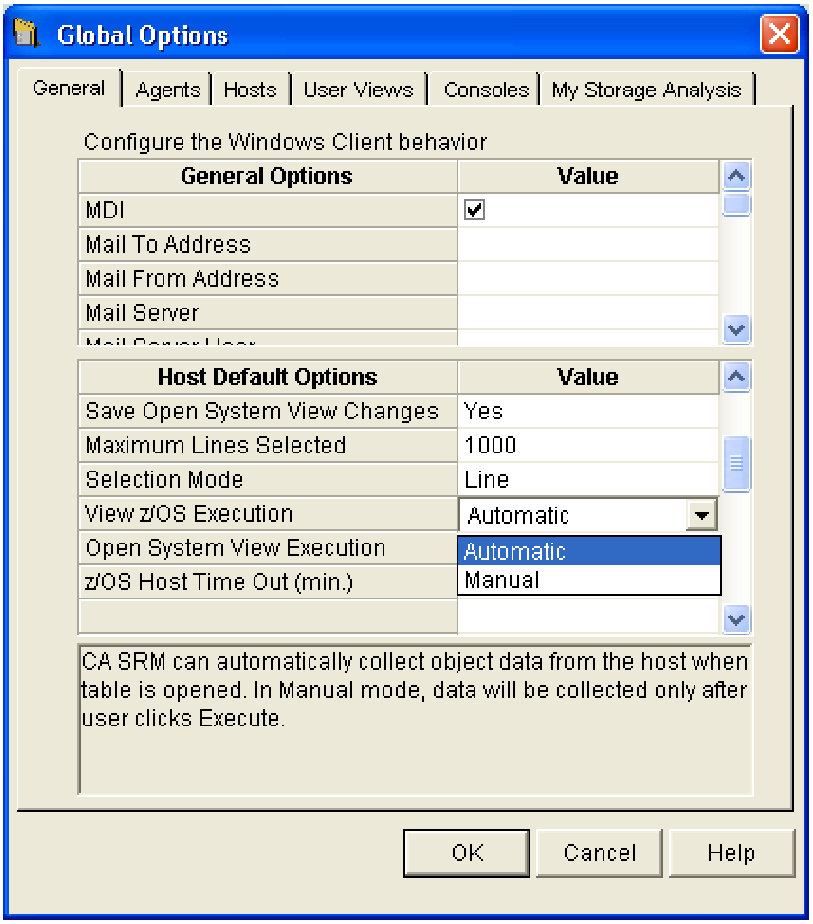
To change the Data Collection mode

1. Click Tools in the Windows Client Main Menu, then select Options, as shown in the following example:



The Global Options dialog opens.

2. On the General tab, select View z/OS Execution, choose the data collection mode that you want to use, and click OK. The following is a sample of the Global Options dialog with the down arrow selected next to View z/OS Execution:



Configure the Windows Client behavior

General Options	Value
MDI	☑
Mail To Address	
Mail From Address	
Mail Server	

Host Default Options	Value
Save Open System View Changes	Yes
Maximum Lines Selected	1000
Selection Mode	Line
View z/OS Execution	Automatic
Open System View Execution	
z/OS Host Time Out (min.)	

CA SRM can automatically collect object data from the host when table is opened. In Manual mode, data will be collected only after user clicks Execute.

The Windows Client will collect data based on the mode that you have chosen. If you select Automatic then the Windows Client will automatically collect object data from the host when an object view is opened. If you select Manual then the Windows Client will only collect object data from the host after you click the Execute icon in the tool bar of the object view.

Note: The examples used in this Guide assume that Automatic mode is selected.

Using Objects to Audit Tape Encryption Processing

The following sections explain how to use objects to audit your CA Tape Encryption processing.

View Tape Encryption Subsystem Address Spaces

The Tape Encryption Subsystem Address Spaces object displays the active CA Tape Encryption Subsystem Address Spaces (also known as BES tasks or BES subsystems) on the z/OS system you are connected to. A single system (LPAR) can accommodate a maximum of eight subsystems.

The Subsystem Address Spaces object is useful in monitoring your CA Tape Encryption environment at a high level. It provides visibility to the BES tasks active on the system and the database and parmlib data sets that they use.

You can use the object to do the following:

- View a new test version of CA Tape Encryption. A new version number for the test subsystem should be displayed in the Tape Encryption Subsystem Address Spaces window. Note that Service Packs typically do not change the version number.
- Confirm what databases and parmlib data sets are in use for each task. A test BES subsystem should have a separate test, primary, and mirror database, and a separate test parmlib.
- Determine if a BES task is restricted to using FIPS-certified encryption routines. (FIPS field is set to Y.)
- Determine if a BES task is configured to interface to the tape management system. (TMS Update field is set to Y.)

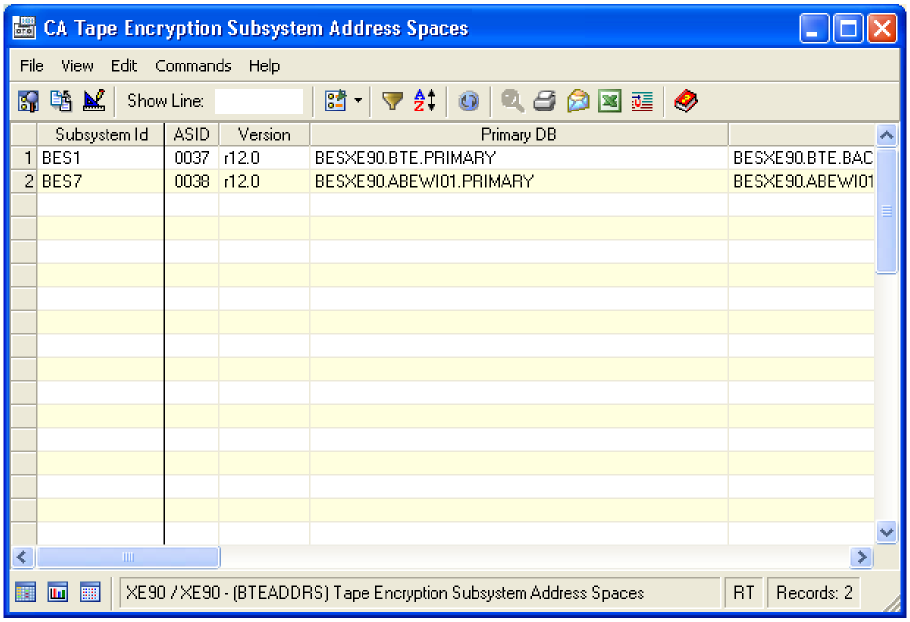
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click on the Subsystem Address Spaces object name in the object tree.

   The Tape Encryption Subsystem Address Spaces window opens, as shown in the following sample:

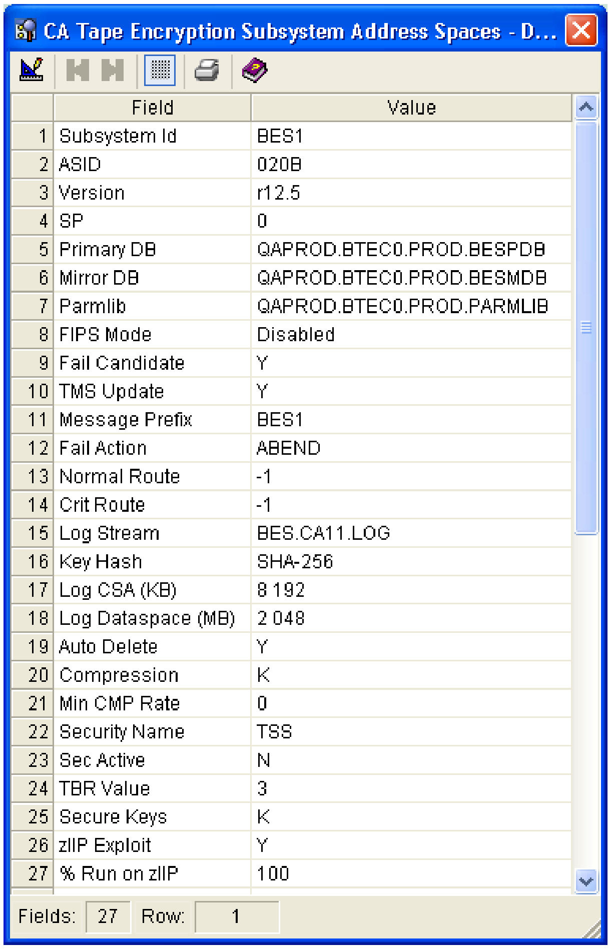


	Subsystem Id	ASID	Version	Primary DB	
1	BES1	0037	r12.0	BESXE90.BTE.PRIMARY	BESXE90.BTE.BAC
2	BES7	0038	r12.0	BESXE90.ABEWI01.PRIMARY	BESXE90.ABEWI01

XE90 / XE90 - (BTEADDRS) Tape Encryption Subsystem Address Spaces | RT | Records: 2

3. To view detailed information associated with a line item, select it, and click the Display detailed line icon.

4. The Tape Encryption Subsystem Address Spaces - Details window opens, as shown in the following sample:



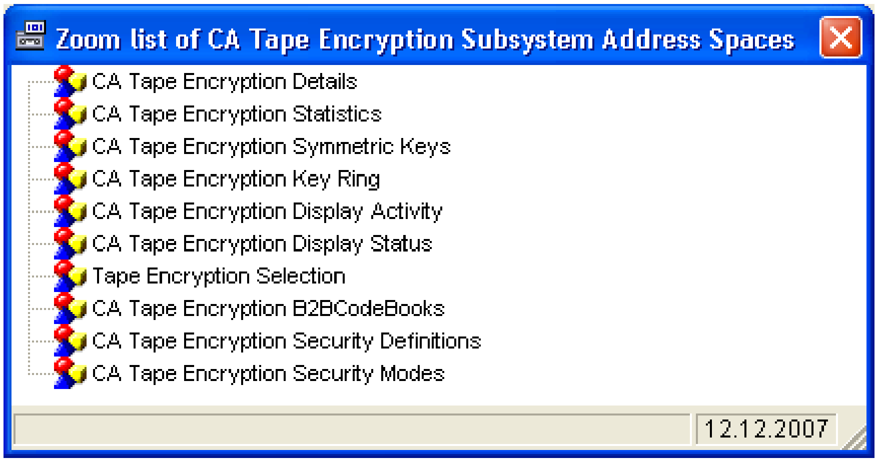
	Field	Value
1	Subsystem Id	BES1
2	ASID	020B
3	Version	r12.5
4	SP	0
5	Primary DB	QAPROD.BTEC0.PROD.BESPDB
6	Mirror DB	QAPROD.BTEC0.PROD.BESMDB
7	Parmlib	QAPROD.BTEC0.PROD.PARMLIB
8	FIPS Mode	Disabled
9	Fail Candidate	Y
10	TMS Update	Y
11	Message Prefix	BES1
12	Fail Action	ABEND
13	Normal Route	-1
14	Crit Route	-1
15	Log Stream	BES.CA11.LOG
16	Key Hash	SHA-256
17	Log CSA (KB)	8 192
18	Log Dataspace (MB)	2 048
19	Auto Delete	Y
20	Compression	K
21	Min CMP Rate	0
22	Security Name	TSS
23	Sec Active	N
24	TBR Value	3
25	Secure Keys	K
26	zIIP Exploit	Y
27	% Run on zIIP	100

Fields: 27 Row: 1

Note: You can get online help that defines each field by clicking the help icon 📖.

5. Double click a line in the Tape Encryption Subsystem Address Spaces table.

   The Zoom list of Tape Encryption Subsystems dialog opens. The Zoom list allows you to select a Tape Encryption object and open a window that displays only the data associated with the selected subsystem, as shown in the following sample:



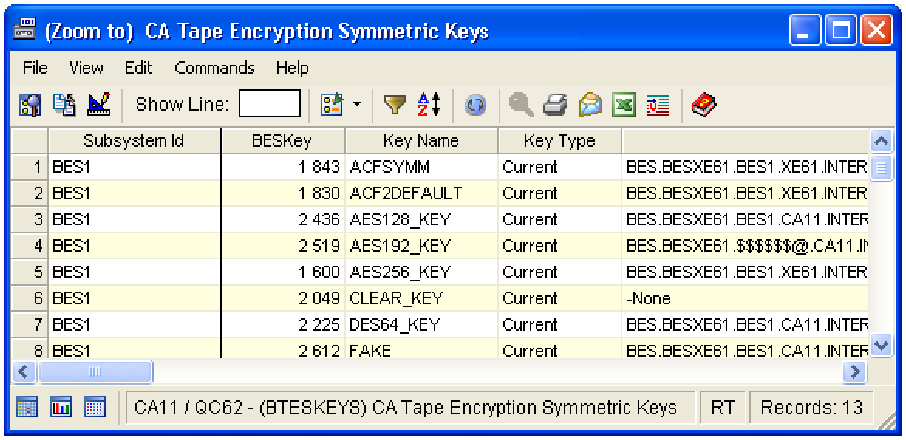
Zoom list of CA Tape Encryption Subsystem Address Spaces

- CA Tape Encryption Details
- CA Tape Encryption Statistics
- CA Tape Encryption Symmetric Keys
- CA Tape Encryption Key Ring
- CA Tape Encryption Display Activity
- CA Tape Encryption Display Status
- Tape Encryption Selection
- CA Tape Encryption B2BCodeBooks
- CA Tape Encryption Security Definitions
- CA Tape Encryption Security Modes

12.12.2007

6. Double-click Tape Encryption Symmetric Keys.

   The Zoom to Tape Encryption Symmetric Keys window opens, displaying the symmetric keys associated with the selected subsystem, as shown in the following sample:



(Zoom to) CA Tape Encryption Symmetric Keys

	Subsystem Id	BESKey	Key Name	Key Type	
1	BES1	1 843	ACFSYMM	Current	BES.BESXE61.BES1.XE61.INTER
2	BES1	1 830	ACF2DEFAULT	Current	BES.BESXE61.BES1.XE61.INTER
3	BES1	2 436	AES128_KEY	Current	BES.BESXE61.BES1.CA11.INTER
4	BES1	2 519	AES192_KEY	Current	BES.BESXE61.$$$$$$@.CA11.IN
5	BES1	1 600	AES256_KEY	Current	BES.BESXE61.BES1.XE61.INTER
6	BES1	2 049	CLEAR_KEY	Current	-None
7	BES1	2 225	DES64_KEY	Current	BES.BESXE61.BES1.CA11.INTER
8	BES1	2 612	FAKE	Current	BES.BESXE61.BES1.CA11.INTER

CA11 / QC62 - (BTESKEYS) CA Tape Encryption Symmetric Keys | RT | Records: 13

You can also use the Filter dialog to display and select elements for a single subsystem. Use the Filter icon on the menu bar to open the Filter dialog.

View Tape Encryption/Decryption Details

The Tape Encryption/Decryption Details window displays detailed information about the most recent 1000 encrypted or decrypted files for each active subsystem. The number of records is limited by a restriction in the BES database that only allows 1000 records per BES task to be stored.

Use the Tape Encryption/Decryption Details window to monitor the specific tape data sets you want to be encrypted and to track those that have been encrypted. The window provides an alternate view of information that is also included in a job log. For example, when you submit an encryption job, the job log will include messages indicating whether a data set was encrypted or decrypted.

After you submit a tape job to create a data set, the Tape Encryption/Decryption Details window will include an entry for that job when it completes. The entry includes the data set name, volume serial number, run date, key name and many more details.

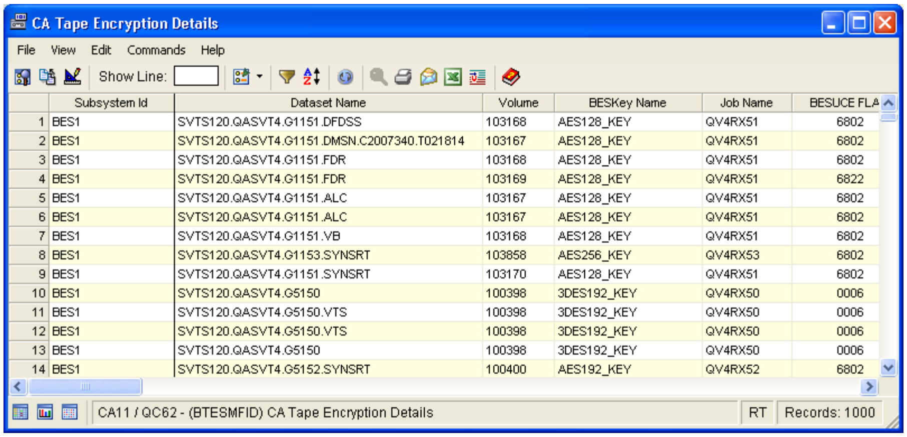
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Tape Encryption Details** object in the object tree.

   The Tape Encryption/Decryption Details window opens, as shown in the following sample:



	Subsystem Id	Dataset Name	Volume	BESKey Name	Job Name	BESUCE FLA
1	BES1	SVTS120.QASVT4.G1151.DFDSS	103168	AES128_KEY	QV4RX51	6802
2	BES1	SVTS120.QASVT4.G1151.DMSN.C2007340.T021814	103167	AES128_KEY	QV4RX51	6802
3	BES1	SVTS120.QASVT4.G1151.FDR	103168	AES128_KEY	QV4RX51	6802
4	BES1	SVTS120.QASVT4.G1151.FDR	103169	AES128_KEY	QV4RX51	6822
5	BES1	SVTS120.QASVT4.G1151.ALC	103167	AES128_KEY	QV4RX51	6802
6	BES1	SVTS120.QASVT4.G1151.ALC	103167	AES128_KEY	QV4RX51	6802
7	BES1	SVTS120.QASVT4.G1151.VB	103168	AES128_KEY	QV4RX51	6802
8	BES1	SVTS120.QASVT4.G1153.SYNSRT	103858	AES256_KEY	QV4RX53	6802
9	BES1	SVTS120.QASVT4.G1151.SYNSRT	103170	AES128_KEY	QV4RX51	6802
10	BES1	SVTS120.QASVT4.G5150	100398	3DES192_KEY	QV4RX50	0006
11	BES1	SVTS120.QASVT4.G5150.VTS	100398	3DES192_KEY	QV4RX50	0006
12	BES1	SVTS120.QASVT4.G5150.VTS	100398	3DES192_KEY	QV4RX50	0006
13	BES1	SVTS120.QASVT4.G5150	100398	3DES192_KEY	QV4RX50	0006
14	BES1	SVTS120.QASVT4.G5152.SYNSRT	100400	AES192_KEY	QV4RX52	6802

CA11 / QC62 - (BTESMFID) CA Tape Encryption Details | RT | Records: 1000

View Tape Encryption/Decryption Statistics

The Tape Encryption/Decryption Statistics window displays high-level encryption and decryption information for subsystems. Use this window to monitor the number of data set encryptions performed to ensure that you do not exceed the license limit. The window provides a month-by-month count of the number of tape file encryptions for the last 12 months. Separate counts are provided for the current month.

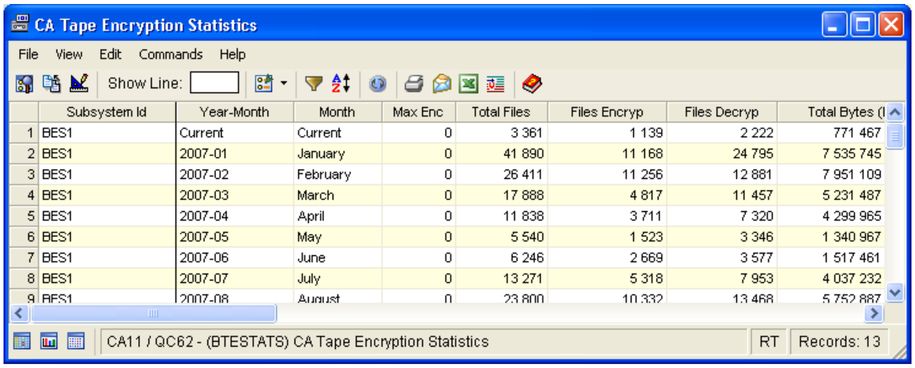
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Statistics** object in the object tree.

   The Tape Encryption/Decryption Statistics window opens, as shown in the following sample:



	Subsystem Id	Year-Month	Month	Max Enc	Total Files	Files Encryp	Files Decryp	Total Bytes (I
1	BES1	Current	Current	0	3 361	1 139	2 222	771 467
2	BES1	2007-01	January	0	41 890	11 168	24 795	7 535 745
3	BES1	2007-02	February	0	26 411	11 256	12 881	7 951 109
4	BES1	2007-03	March	0	17 888	4 817	11 457	5 231 487
5	BES1	2007-04	April	0	11 838	3 711	7 320	4 299 965
6	BES1	2007-05	May	0	5 540	1 523	3 346	1 340 967
7	BES1	2007-06	June	0	6 246	2 669	3 577	1 517 461
8	BES1	2007-07	July	0	13 271	5 318	7 953	4 037 232
9	BES1	2007-08	August	0	23 800	10 332	13 468	5 752 887

CA11 / QC62 - (BTESTATS) CA Tape Encryption Statistics | RT | Records: 13

View Tape Encryption Symmetric Keys

The Tape Encryption Symmetric Keys window displays the current key instance for each key defined to the active subsystems. The window includes a number of useful fields that are captured from the Symmetric Keys definitions in parmlib, including Key Name, Key Type, Key Index, Number of Generations, Algorithm used, How often the key is regenerated (Weekly, Monthly or Yearly), and Date the key was generated. To view all symmetric key details scroll right and left.

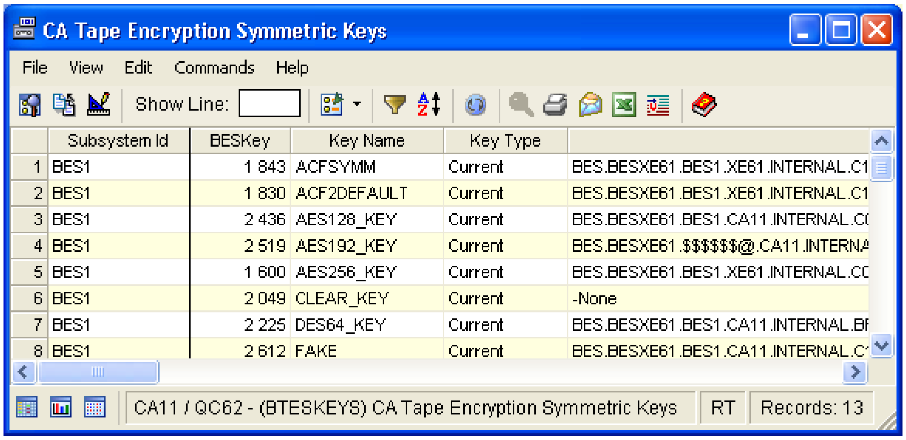
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Symmetric Keys** object in the object tree.

   The Tape Encryption Symmetric Keys object opens as shown in the following sample:

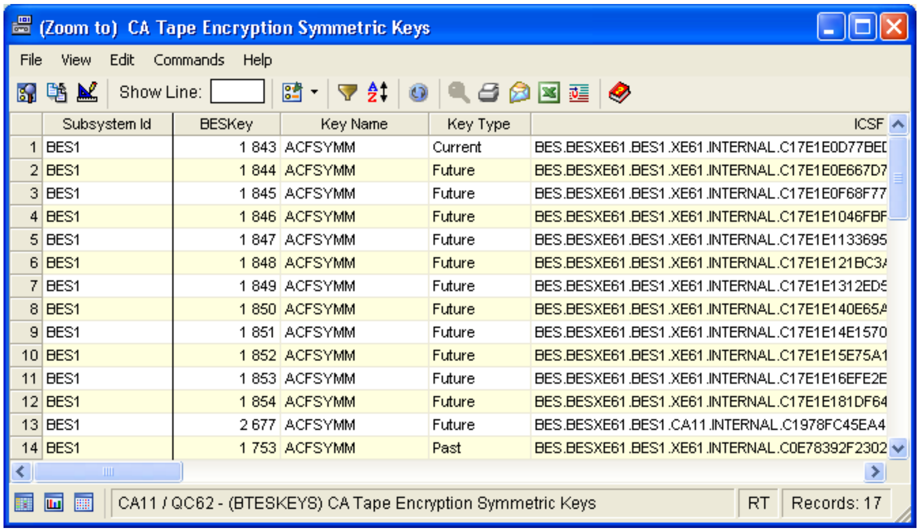


	Subsystem Id	BESKey	Key Name	Key Type	
1	BES1	1 843	ACFSYMM	Current	BES.BESXE61.BES1.XE61.INTERNAL.C1
2	BES1	1 830	ACF2DEFAULT	Current	BES.BESXE61.BES1.XE61.INTERNAL.C1
3	BES1	2 436	AES128_KEY	Current	BES.BESXE61.BES1.CA11.INTERNAL.C
4	BES1	2 519	AES192_KEY	Current	BES.BESXE61.$$$$$$@.CA11.INTERNA
5	BES1	1 600	AES256_KEY	Current	BES.BESXE61.BES1.XE61.INTERNAL.C
6	BES1	2 049	CLEAR_KEY	Current	-None
7	BES1	2 225	DES64_KEY	Current	BES.BESXE61.BES1.CA11.INTERNAL.B
8	BES1	2 612	FAKE	Current	BES.BESXE61.BES1.CA11.INTERNAL.C

CA11 / QC62 - (BTESKEYS) CA Tape Encryption Symmetric Keys | RT | Records: 13

3. To view all generations of a specific key, double click the table row containing the key.

   The (Zoom to) Tape Encryption Symmetric Keys window opens displaying all generations of the selected key. For example, if you have requested that 7 generations of a key be always kept in advance, the window displays at least 8 key instances. The first key in the table is the Current key, followed by Future and Past keys. The following is a sample of the (Zoom to) Tape Encryption Symmetric Keys window:



	Subsystem Id	BESKey	Key Name	Key Type	ICSF
1	BES1	1 843	ACFSYMM	Current	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E0D77BED
2	BES1	1 844	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E0E667D7
3	BES1	1 845	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E0F68F77
4	BES1	1 846	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E1046FBF
5	BES1	1 847	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E1133695
6	BES1	1 848	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E121BC3A
7	BES1	1 849	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E1312ED5
8	BES1	1 850	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E140E65A
9	BES1	1 851	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E14E1570
10	BES1	1 852	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E15E75A1
11	BES1	1 853	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E16EFE2E
12	BES1	1 854	ACFSYMM	Future	BES.BESXE61.BES1.XE61.INTERNAL.C17E1E181DF64
13	BES1	2 677	ACFSYMM	Future	BES.BESXE61.BES1.CA11.INTERNAL.C1978FC45EA4
14	BES1	1 753	ACFSYMM	Past	BES.BESXE61.BES1.XE61.INTERNAL.C0E78392F2302

CA11 / QC62 - (BTESKEYS) CA Tape Encryption Symmetric Keys | RT | Records: 17

View Tape Encryption Key Rings

The Tape Encryption Key Ring window displays all the key rings for all subsystems. It displays the Key Rings defined through your external security system, including the digital certificates CA Tape Encryption uses in creating B2B tapes. Key Rings are created, protected, and managed by the external security system. Use this window to display the names of the Key Rings that contain the digital certificates used by CA Tape Encryption. To access the digital certificates you must use the facilities provided by your security system.

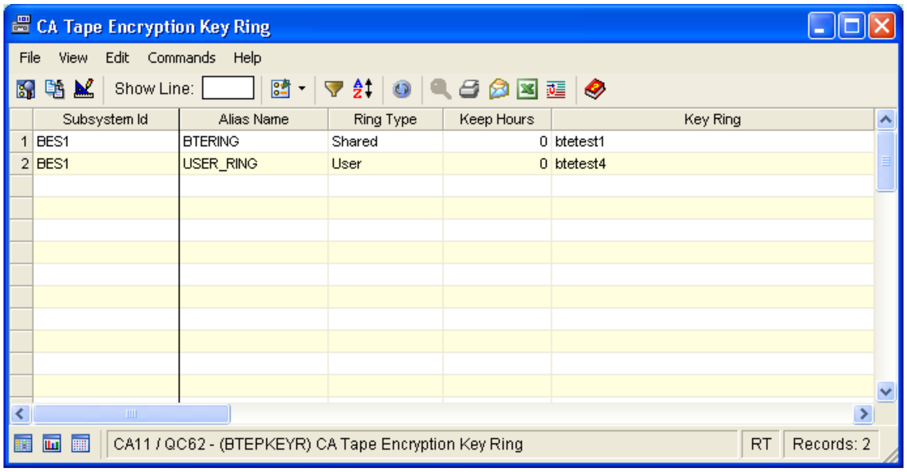
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Key Rings** object in the object tree.

   The Tape Encryption Key Ring window opens, as shown in the following sample:

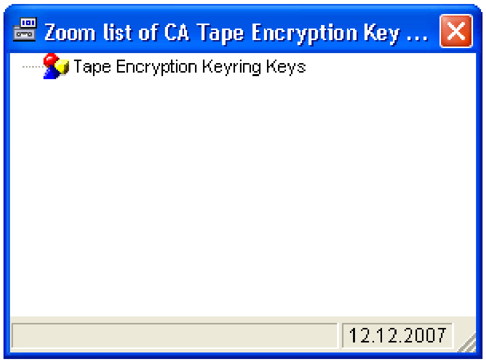


	Subsystem Id	Alias Name	Ring Type	Keep Hours	Key Ring
1	BES1	BTERING	Shared	0	btetest1
2	BES1	USER_RING	User	0	btetest4

CA11 / QC62 - (BTEPKEYR) CA Tape Encryption Key Ring RT Records: 2

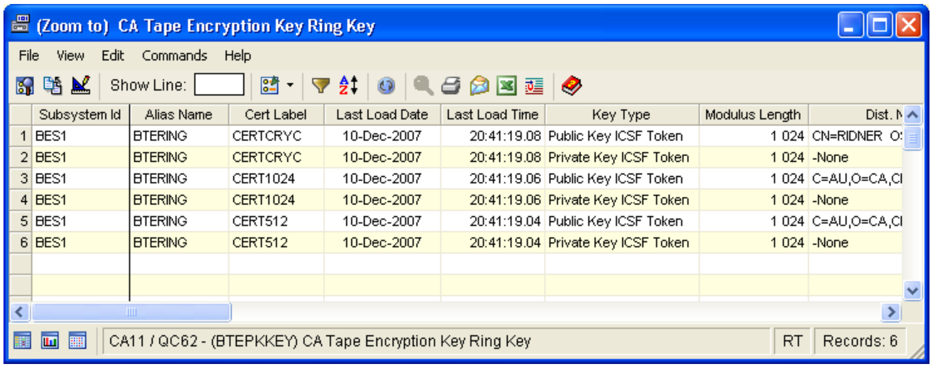
3. Select a key ring and click the **Open Zoom** button.

   The Zoom list of Tape Encryption Key Ring dialog opens, as shown in the following sample:


Zoom list of CA Tape Encryption Key ...
Tape Encryption Keyring Keys
12.12.2007

4. Double-click the Tape Encryption Keyring Keys item.

   The (Zoom to) Tape Encryption Key Ring Key dialog opens. This display provides additional details about the selected key ring, such as its key type and module length, as shown in the following sample:



	Subsystem Id	Alias Name	Cert Label	Last Load Date	Last Load Time	Key Type	Modulus Length	Dist. N
1	BES1	BTERING	CERTCRYC	10-Dec-2007	20:41:19.08	Public Key ICSF Token	1 024	CN=RIDNER O:
2	BES1	BTERING	CERTCRYC	10-Dec-2007	20:41:19.08	Private Key ICSF Token	1 024	-None
3	BES1	BTERING	CERT1024	10-Dec-2007	20:41:19.06	Public Key ICSF Token	1 024	C=AU,O=CA,CI
4	BES1	BTERING	CERT1024	10-Dec-2007	20:41:19.06	Private Key ICSF Token	1 024	-None
5	BES1	BTERING	CERT512	10-Dec-2007	20:41:19.04	Public Key ICSF Token	1 024	C=AU,O=CA,CI
6	BES1	BTERING	CERT512	10-Dec-2007	20:41:19.04	Private Key ICSF Token	1 024	-None

CA11 / QC62 - (BTEPKKEY) CA Tape Encryption Key Ring Key | RT | Records: 6

View Tape Encryption/Decryption Display Activity

The Tape Encryption/Decryption Display Activity window displays the jobs running on the system for which CA Tape Encryption is currently performing decryption or encryption.

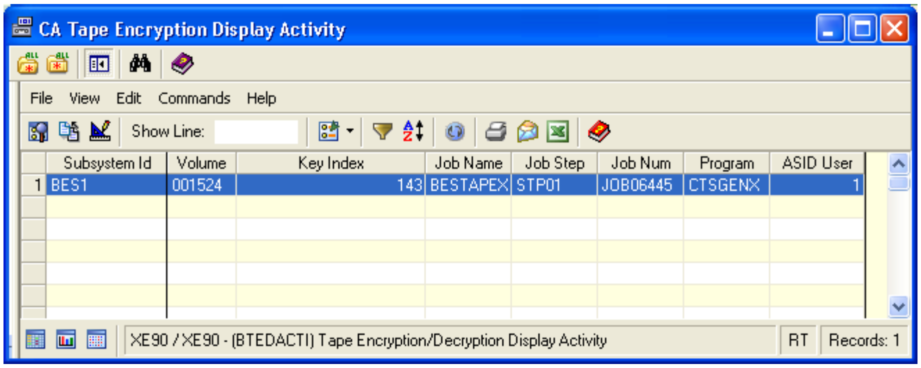
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Display Activity** object in the object tree.

   The Tape Encryption/Decryption Display Activity window opens, as shown in the following sample:



	Subsystem Id	Volume	Key Index	Job Name	Job Step	Job Num	Program	ASID User
1	BES1	001524	143	BESTAPEX	STP01	JOB06445	CTSGENX	1

XE90 / XE90 - (BTEDACTI) Tape Encryption/Decryption Display Activity | RT | Records: 1

Note: If there are no jobs currently running that require encryption or decryption processing, the display will be empty.

View Tape Encryption/Decryption Display Status

The Tape Encryption/Decryption Display Status window displays the status of all the parameters and details of the cryptographic environment for each subsystem. It displays the same information as the display status command. Among other things, the display provides information about:

- The ICSF environment
- Crypto processors on the system
- Tape management system interface routines
- The level of shared CA Tape Encryption routines

  Note: The routines are shared because all active address spaces use them.

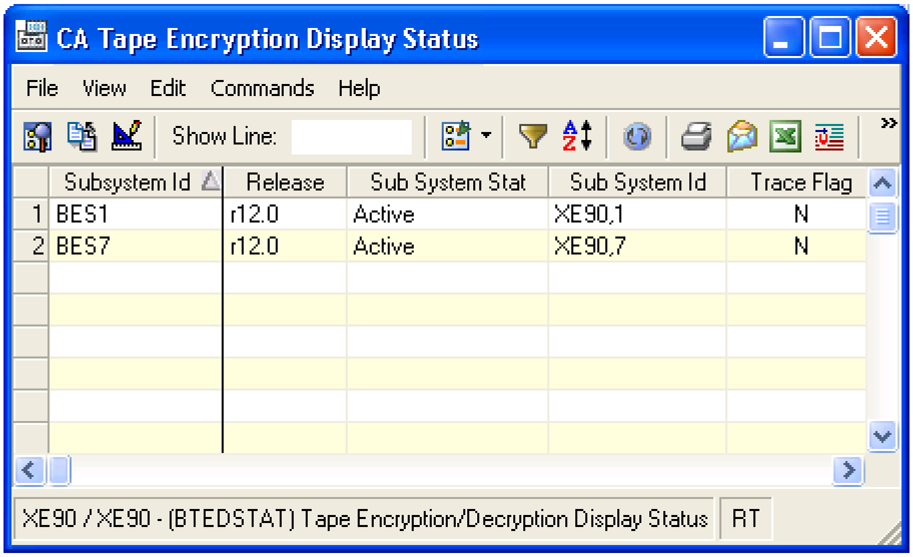
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Display Status** object in the object tree.

   The Tape Encryption/Decryption Display Status window opens, as shown in the following sample:

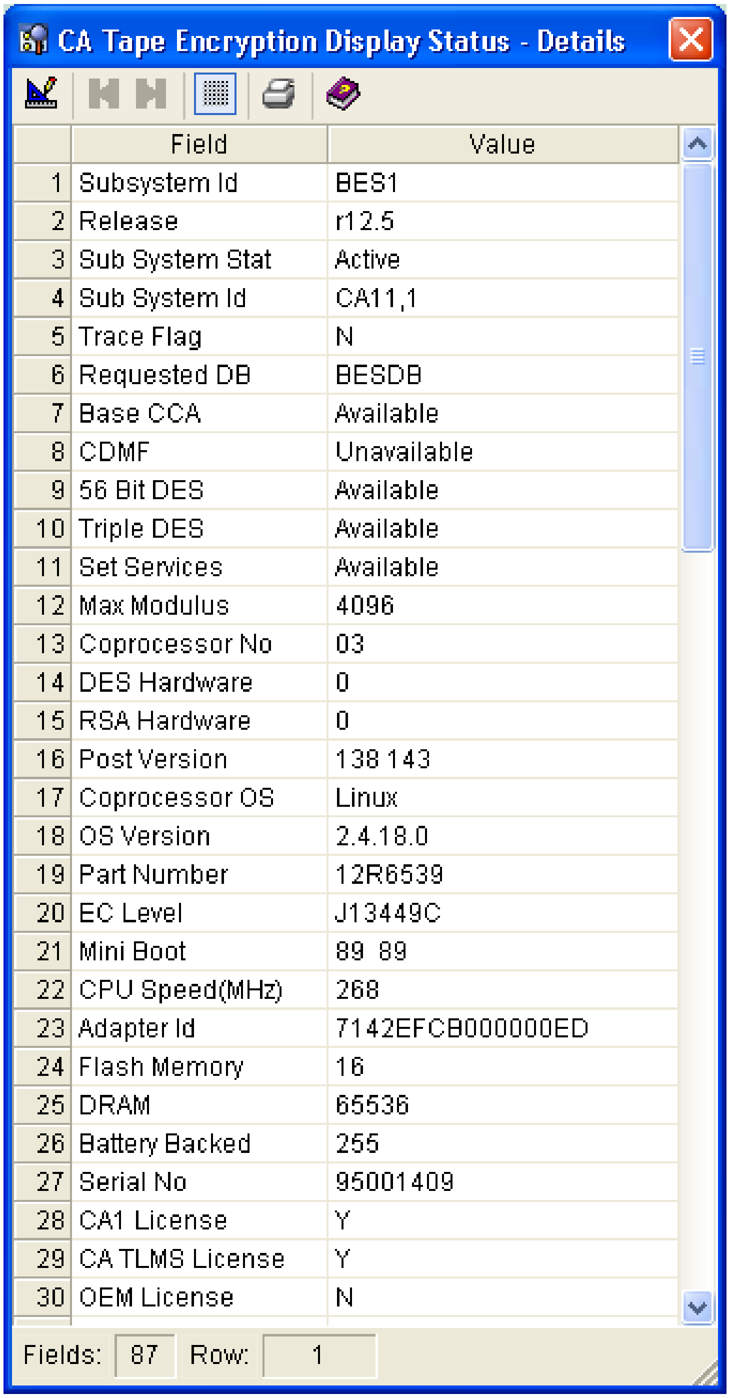

CA Tape Encryption Display Status
File View Edit Commands Help
Show Line:

	Subsystem Id	Release	Sub System Stat	Sub System Id	Trace Flag
1	BES1	r12.0	Active	XE90,1	N
2	BES7	r12.0	Active	XE90,7	N

XE90 / XE90 - (BTEDSTAT) Tape Encryption/Decryption Display Status | RT

3. Use the Display detailed line icon to view detailed information associated with a line item.

   The Tape Encryption/Decryption Display Status - Details window opens, as shown in the following sample:



CA Tape Encryption Display Status - Details

	Field	Value
1	Subsystem Id	BES1
2	Release	r12.5
3	Sub System Stat	Active
4	Sub System Id	CA11,1
5	Trace Flag	N
6	Requested DB	BESDB
7	Base CCA	Available
8	CDMF	Unavailable
9	56 Bit DES	Available
10	Triple DES	Available
11	Set Services	Available
12	Max Modulus	4096
13	Coprocessor No	03
14	DES Hardware	0
15	RSA Hardware	0
16	Post Version	138 143
17	Coprocessor OS	Linux
18	OS Version	2.4.18.0
19	Part Number	12R6539
20	EC Level	J13449C
21	Mini Boot	89 89
22	CPU Speed(MHz)	268
23	Adapter Id	7142EFCB000000ED
24	Flash Memory	16
25	DRAM	65536
26	Battery Backed	255
27	Serial No	95001409
28	CA1 License	Y
29	CA TLMS License	Y
30	OEM License	N

Fields: 87 Row: 1

View Encryption Selection Information

The Encryption Selection window displays criteria used to select datasets to be encrypted. This information can come from the SMS data classes with appropriate encryption keywords described in the description field or from the external security system where profiles beginning with “DSN.” have been defined.

The Encryption Selection object can help you troubleshoot data set set selection problems. For instance, if you set up a data class but misspell a key name, so that the name does not match any of the keys in the CA Tape Encryption parmlib, you can use this display to check the key name spelling. Similarly, you can use this display to verify the external security system definitions for selection, verifying the dataset name and the CA Tape Encryption keywords associated with the security profile.

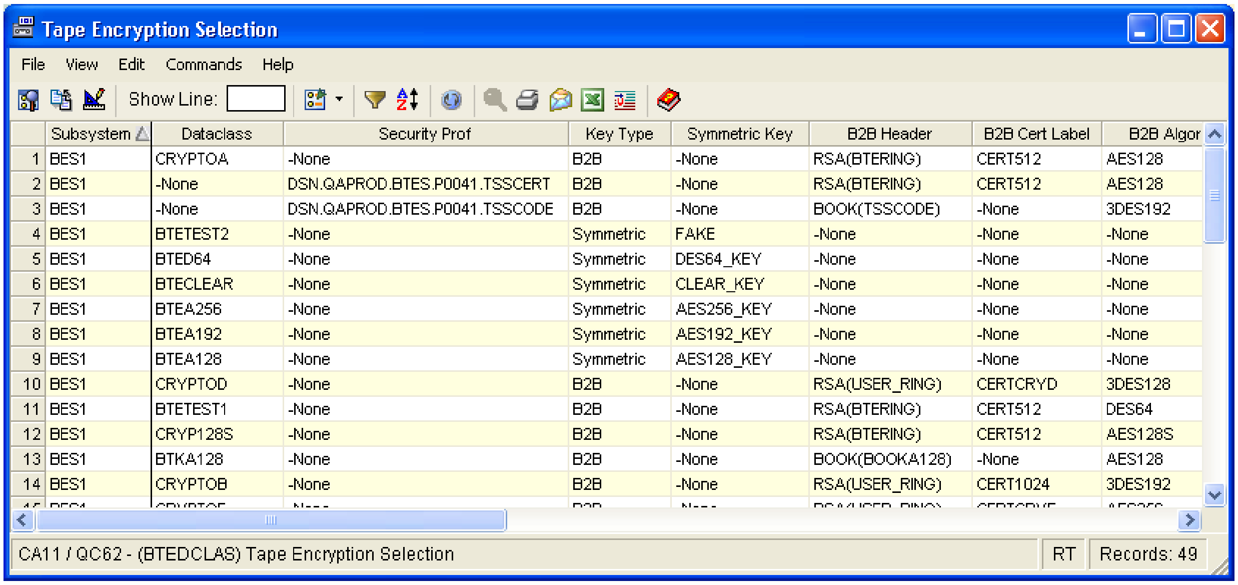
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Encryption Selection** object tree.

   The EncryptionSelection window opens, as shown in the following sample:



	Subsystem	Dataclass	Security Prof	Key Type	Symmetric Key	B2B Header	B2B Cert Label	B2B Algor
1	BES1	CRYPTOA	-None	B2B	-None	RSA(BTERING)	CERT512	AES128
2	BES1	-None	DSN.QAPROD.BTES.P0041.TSSCERT	B2B	-None	RSA(BTERING)	CERT512	AES128
3	BES1	-None	DSN.QAPROD.BTES.P0041.TSSCODE	B2B	-None	BOOK(TSSCODE)	-None	3DES192
4	BES1	BTETEST2	-None	Symmetric	FAKE	-None	-None	-None
5	BES1	BTED64	-None	Symmetric	DES64_KEY	-None	-None	-None
6	BES1	BTECLEAR	-None	Symmetric	CLEAR_KEY	-None	-None	-None
7	BES1	BTEA256	-None	Symmetric	AES256_KEY	-None	-None	-None
8	BES1	BTEA192	-None	Symmetric	AES192_KEY	-None	-None	-None
9	BES1	BTEA128	-None	Symmetric	AES128_KEY	-None	-None	-None
10	BES1	CRYPTOD	-None	B2B	-None	RSA(USER_RING)	CERTCRYD	3DES128
11	BES1	BTETEST1	-None	B2B	-None	RSA(BTERING)	CERT512	DES64
12	BES1	CRYP128S	-None	B2B	-None	RSA(BTERING)	CERT512	AES128S
13	BES1	BTKA128	-None	B2B	-None	BOOK(BOOKA128)	-None	AES128
14	BES1	CRYPTOB	-None	B2B	-None	RSA(USER_RING)	CERT1024	3DES192

CA11 / QC62 - (BTEDCLAS) Tape Encryption Selection | RT | Records: 49

View Tape Encryption B2BCodeBooks Information

The Tape Encryption B2BCodeBooks dialog displays all the B2B code books you have defined in the B2BBOOKS parmlib member, and which have been loaded into the CA Tape Encryption database. B2B code books are used to encrypt tapes for use on distributed systems.

The B2BCodeBooks display is useful in determining if a distributed system has the most recent code book available. The display presents a complete list of the code books defined to all BES tasks sharing the CA Tape Encryption database. Before they can be sent to a distributed system, the code books must be exported using the TBEBOOK utility, which formats them for transmission to a distributed system. The B2BcodeBooks dialog displays the time and date that a code book was exported. Using this time and date information, you can check that a distributed system has the current code book.

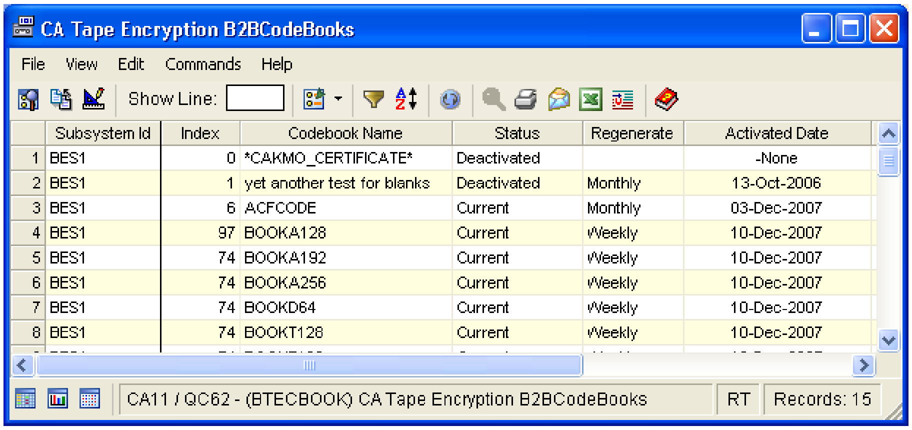
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **B2BCodeBooks** object in the object tree.

   The B2BCodeBooks window opens, as shown in the following sample:



	Subsystem Id	Index	Codebook Name	Status	Regenerate	Activated Date
1	BES1	0	*CAKMO_CERTIFICATE*	Deactivated		-None
2	BES1	1	yet another test for blanks	Deactivated	Monthly	13-Oct-2006
3	BES1	6	ACFCODE	Current	Monthly	03-Dec-2007
4	BES1	97	BOOKA128	Current	Weekly	10-Dec-2007
5	BES1	74	BOOKA192	Current	Weekly	10-Dec-2007
6	BES1	74	BOOKA256	Current	Weekly	10-Dec-2007
7	BES1	74	BOOKD64	Current	Weekly	10-Dec-2007
8	BES1	74	BOOKT128	Current	Weekly	10-Dec-2007

CA11 / QC62 - (BTECBOOK) CA Tape Encryption B2BCodeBooks | RT | Records: 15

View Security Definitions Information

The Security Definitions window displays all items defined to the external security system that affect the operation of CA Tape Encryption. These definitions include data set selection profiles, command protection profiles, utility protection profiles, key protection profiles, and default control profiles. Profiles that will apply to all CA Tape Encryption address spaces are prefixed with “BES.”, and specific profiles that apply to an individual CA Tape Encryption address space begin with “BES” followed by the number of the address space, such as “BES1”. Data set selection profiles begin with “DSN.” followed by the data set name.

For example, all data sets that will be selected for encryption using the security feature will have a “Resource Type” of “Dataset Selection”.

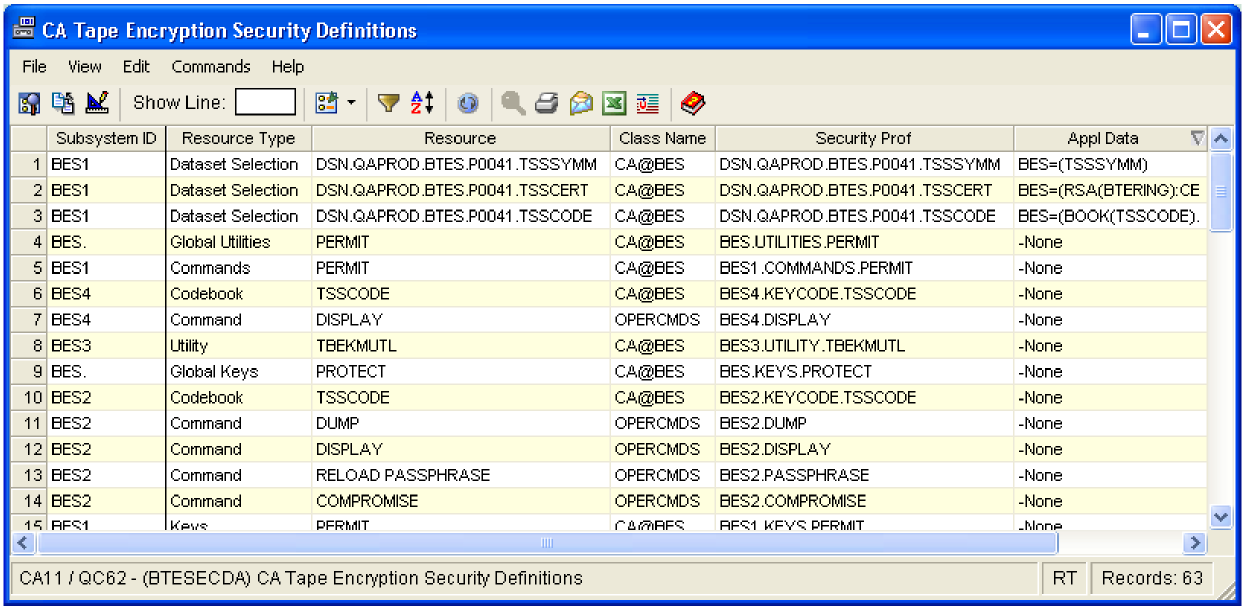
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the Security Definitions object tree.

   The Security Definitions window opens, as shown in the following sample:



	Subsystem ID	Resource Type	Resource	Class Name	Security Prof	Appl Data
1	BES1	Dataset Selection	DSN.QAPROD.BTES.P0041.TSSSYMM	CA@BES	DSN.QAPROD.BTES.P0041.TSSSYMM	BES=(TSSSYMM)
2	BES1	Dataset Selection	DSN.QAPROD.BTES.P0041.TSSCERT	CA@BES	DSN.QAPROD.BTES.P0041.TSSCERT	BES=(RSA(BTERING):CE
3	BES1	Dataset Selection	DSN.QAPROD.BTES.P0041.TSSCODE	CA@BES	DSN.QAPROD.BTES.P0041.TSSCODE	BES=(BOOK(TSSCODE).
4	BES.	Global Utilities	PERMIT	CA@BES	BES.UTILITIES.PERMIT	-None
5	BES1	Commands	PERMIT	CA@BES	BES1.COMMANDS.PERMIT	-None
6	BES4	Codebook	TSSCODE	CA@BES	BES4.KEYCODE.TSSCODE	-None
7	BES4	Command	DISPLAY	OPERCMDS	BES4.DISPLAY	-None
8	BES3	Utility	TBEKMUTL	CA@BES	BES3.UTILITY.TBEKMUTL	-None
9	BES.	Global Keys	PROTECT	CA@BES	BES.KEYS.PROTECT	-None
10	BES2	Codebook	TSSCODE	CA@BES	BES2.KEYCODE.TSSCODE	-None
11	BES2	Command	DUMP	OPERCMDS	BES2.DUMP	-None
12	BES2	Command	DISPLAY	OPERCMDS	BES2.DISPLAY	-None
13	BES2	Command	RELOAD PASSPHRASE	OPERCMDS	BES2.PASSPHRASE	-None
14	BES2	Command	COMPROMISE	OPERCMDS	BES2.COMPROMISE	-None
15	BES1	Keys	PERMIT	CA@BES	BES1.KEYS.PERMIT	-None

CA11 / QC62 - (BTESECDA) CA Tape Encryption Security Definitions | RT | Records: 63

View Security Modes Information

The Security Modes window displays the default security modes for each active CA Tape Encryption address space. The modes are displayed for commands, keys, and utilities. You can see at a glance how security is implemented for each active CA Tape Encryption address space. “Protected” and “Protected Global” indicate a security profile is needed to access the resource. “Permitted” and “Permitted Global” indicate that access to a resource will be permitted if no security profile for the resource exists.

For example, a production CA Tape Encryption address space might show “Protected” or “Protected Global” for each resource type, while a test CA Tape Encryption address might show “Permitted” or “Permitted Global” for the resources. This display is useful in determining what resources are protected or permitted for any active CA Tape Encryption address space. If “BES.DEFAULT” appears as “Y”, reference the “Security Definitions” object to determine what action has been defined for BES.DEFAULT.

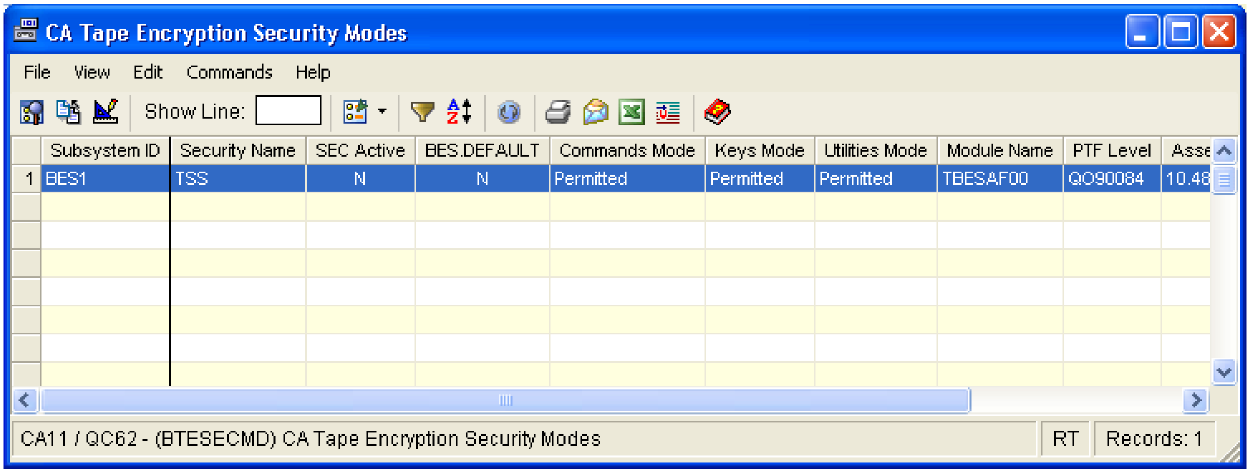
To open the display

1. Open the Object Tree and find the Tape Encryption objects as described in the Access CA Tape Encryption Objects from the Windows Client section.

   The Object Tree is displayed in the Windows Client showing the CA Tape Encryption objects.

2. Click the **Security Modes** object tree.

   The Security Mode window opens, as shown in the following sample:



	Subsystem ID	Security Name	SEC Active	BES.DEFAULT	Commands Mode	Keys Mode	Utilities Mode	Module Name	PTF Level	Asse
1	BES1	TSS	N	N	Permitted	Permitted	Permitted	TBESAF00	QO90084	10.48

CA11 / QC62 - (BTESECMD) CA Tape Encryption Security Modes | RT | Records: 1

Chapter 3: Verifying CA Tape Encryption

This section contains the following topics:

Dump an Encrypted Tape

You may want to routinely dump encrypted tapes to verify that CA Tape Encryption is processing as expected. The IDCAMS utility, available in every z/OS system, provides multiple ways to dump the tape to verify its contents. CA Tape Encryption dynamically changes Standard Label (SL) tapes to Standard User Label (SUL) tapes to retain information on the encryption type and other data used to track and manage the encryption keys associated with the tape.

You can choose to dump:

- Only the encrypted tape data
- The encrypted tape data, labels, user header labels, and user trailer labels

Both options are described below.

Dump Encrypted Data

To verify that encrypted data is being processed correctly, use the sample IDCAMS JCL shown below and modify it for your site as appropriate.

Sample IDCAMS JCL to Dump Encrypted Data

```
//*
//STEP1    EXEC PGM=IDCAMS,REGION=4096K
//SYSUT1   DD  DISP=OLD,DSN=your.data.set.name,
//         RECFM=U,BLKSIZE=32760,
//         LABEL=(1,SUL,EXPDT=98000),
//         UNIT=uuuuuuuu,VOL=(,RETAIN,SER=vvvvvv)
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
  PRINT INFILE(SYSUT1) COUNT(nnn)
/*
```

//

Note: While the tape was originally created as an SL tape, SUL is specified to direct IDCAMS to process the User Header Labels (UHLs) correctly.

To dump encrypted data

1. Replace *your.data.set.name* with the name of the encrypted file on the tape that you want to dump.
2. Replace *uuuuuuuu* with a valid unit address or generic unit name in use at your site.
3. Replace *vvvvvv* with the volser of the tape containing the encrypted file specified in STEP1 of the sample.

Note: You can use the COUNT parameter to control the number of data blocks printed in dump format. To do this, change *nnn* to an appropriate numeric value to limit excessive print output.

Dump Tape and File Labels

Use the following sample JCL to dump the tape file labels before and after the data file. This technique uses Bypass Label Processing (BLP) which requires additional security permissions to use. The first step dumps the volume, file headers, and User Header Labels. The second step dumps the data file. The third step dumps the End of Volume, End of File, and User Trailer Labels that follow the data file. The data set names do not need to be changed because of BLP processing.

Sample JCL to Dump Tape and File Labels

```
//*
//HEADER1  EXEC PGM=IDCAMS,REGION=4096K
//SYSUT1   DD  DISP=OLD,DSN=BLP.HEADERS,
//         RECFM=FB,LRECL=80,BLKSIZE=80,
//         LABEL=(1,BLP,EXPDT=98000),
//         UNIT=uuuuuuuu,VOL=(,RETAIN,SER=vvvvvv)
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
  PRINT INFILE(SYSUT1)
/*
//*
//FILE1    EXEC PGM=IDCAMS,REGION=4096K
//SYSUT1   DD  DISP=OLD,DSN=BLP.FILE1,
//         RECFM=U,BLKSIZE=32760,
//         LABEL=(2,BLP,EXPDT=98000),UNIT=uuuuuuuu,
//         VOL=(,RETAIN,SER=vvvvvv)
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
  PRINT INFILE(SYSUT1) COUNT(nnn)
/*
//*
//TRAILER1 EXEC PGM=IDCAMS,REGION=4096K
//SYSUT1   DD  DISP=OLD,DSN=BLP.TRAILERS,
//         RECFM=FB,LRECL=80,BLKSIZE=80,
//         LABEL=(3,BLP,EXPDT=98000),UNIT=uuuuuuuu,
//         VOL=(,RETAIN,SER=vvvvvv)
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
  PRINT INFILE(SYSUT1)
/*
//
```

This JCL is provided in the CTAPJCL data set member BESPRTTP.

To dump tape and file labels

1. Replace *uuuuuuuu* with a valid unit address or generic unit name in use at your site.
2. Replace *vvvvvv* with the volser of the tape containing the encrypted file specified in HEADER1 in the first step of the sample JCL.

Note: You can use the COUNT parameter to control the number of data blocks printed in dump format. To do this, change *nnn* to an appropriate numeric value to limit excessive print output.

Sample Dumped Tape Header Report

```
LISTING OF DATA SET -BLP.HEADERS




 RECORD SEQUENCE NUMBER - 1

 000000  E5D6D3F1 F0F0F1F5 F0F64040 40404040   40404040 40404040 40404040 40404040   *VOL1001506                      *

 000020  40404040 40404040 40404040 40404040   40404040 40404040 40404040 40404040   *                                *

 000040  40404040 40404040 40404040 40404040                                         *                                *




 RECORD SEQUENCE NUMBER - 2

 000000  C8C4D9F1 C9F0F14B C5D5C3D9 E8D7E34B   E5D1F1F9 F2F0F0F1 F5F0F6F0 F0F0F1F0   *HDR1I01.ENCRYPT.VJ19200150600010*

 000020  F0F0F140 40404040 40F0F0F6 F1F0F9F0   F0F0F0F0 F0F0F0F0 F0F0F0F0 C2E3C540   *001      0061090000000000000BTE *

 000040  99F1F24B F00000C0 0D404040 40404040                                         *.12.0..{.                       *




 RECORD SEQUENCE NUMBER - 3

 000000  C8C4D9F2 C6F0F0F0 F8F0F0F0 F0F8F0F0   F0C2C5E2 E3C1D7C5 E761E2E3 D7F0F140   *HDR2F000800008000BESTAPEX/STP01 *

 000020  40404040 4040C240 4040F4F7 F0F0F040   40404040 40404040 40404040 40404040   *      B   47000                 *

 000040  40404040 40404040 40404040 40404040                                         *                                *




 RECORD SEQUENCE NUMBER - 4

 000000  E4C8D3F1 00C4C2C3 F0F099F1 F24BF040   4040F704 02010000 0000C00D 2087D77B   *UHL1.DBC00.12.0   7.......{...P#*

 000020  DF307ACA 14EB2BD9 41555E3F EEF1F80E   01DC69F1 1B114082 D4F2B54C C2E2F0F0   *..:....R..;..18....1.. .M2.<BS00*

 000040  C0000000 00000010 CE758706 6D4F4C5E                                         *{..........._|<;                *




 RECORD SEQUENCE NUMBER - 5
```

```
000000  E4C8D3F2 D7D68677 70B86046 00000000   00000000 00000000 00000000 C1C5E2F1   *UHL2PO....-.................AES1*

000020  F2F84040 40404040 40404040 40404040   40404040 40404040 40404040 C2C5E24B   *28                          BES.*

000040  C2C5E2E6 C7C14BC2 C5E2F74B E7C5F9F0                                         *BESWGA.BES7.XE90                *




RECORD SEQUENCE NUMBER - 6

000000  E4C8D3F3 4BC9D5E3 C5D9D5C1 D34BC2C5   F9C1C6F2 C1F5C1C4 C4C1F1F2 F1F84040   *UHL3.INTERNAL.BE9AF2A5ADDA1218  *

000020  40404040 40404040 40404040 40404040   00000000 00000000 00000000 00000000   *                ................*

000040  00000000 00000000 00000000 00000000                                         *................                *




RECORD SEQUENCE NUMBER - 7

000000  E4C8D3F4 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *UHL4............................*

000020  00000000 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *................................*

000040  00000000 00000000 00000000 00000000                                         *................                *




RECORD SEQUENCE NUMBER - 8

000000  E4C8D3F5 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *UHL5............................*

000020  00000000 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *................................*

000040  00000000 00000000 00000000 00000000                                         *................                *




RECORD SEQUENCE NUMBER - 9

000000  E4C8D3F6 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *UHL6............................*

000020  00000000 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *................................*

000040  00000000 00000000 00000000 00000000                                         *................                *
```

```
RECORD SEQUENCE NUMBER - 10

000000  E4C8D3F7 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *UHL7............................*

000020  00000000 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *................................*

000040  00000000 00000000 00000000 00000000                                         *................                *




RECORD SEQUENCE NUMBER - 11

000000  E4C8D3F8 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *UHL8............................*

000020  00000000 00000000 00000000 00000000   00000000 00000000 00000000 00000000   *................................*

000040  00000000 00000000 00000000 00000000                                         *................                *
```

The unique signature which identifies this tape file as containing data encrypted by CA Tape Encryption is highlighted in the above report sample. The eight user labels, records 4 through 11, provide information about the encryption performed on the file.

Index