Implementing Security for MAINVIEW® Products

December 15, 2000

bmcsoftware

Copyright © 2000 BMC Software, Inc., as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc. IBM and DB2 are registered trademarks of International Business Machines Corp. All other registered trademarks or trademarks belong to their respective companies.

Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. UNPUBLISHED–RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in FAR Section 52.227-14 Alt. III (g)(3), FAR Section 52.227-19, DFARS 252.227-7014 (b), or DFARS 227.7202, as amended from time to time. Send any contract notices to Contractor/Manufacturer:

BMC Software, Inc.
2101 CityWest Blvd.
Houston TX 77042-2827
USA

Contacting BMC Software

You can access the BMC Software Web site at **http://www.bmc.com**. From this Web site, you can obtain general information about the company, its products, special events, and career opportunities. For a complete list of all BMC Software offices and locations, go to **http://www.bmc.com/corporate/offices.html**.

USA and Canada

Address	BMC Software, Inc. 2101 CityWest Blvd. Houston TX 77042-2827
Telephone	713 918 8800 or 800 841 2031
Fax	713 918 8000

Outside USA and Canada

Telephone	(01) 713 918 8800
Fax	(01) 713 918 8000

Customer Support

You can obtain technical support by using Response Online™ (comprehensive information from the Web) or Response On Demand™. To expedite your inquiry, please see “Before Contacting BMC Software,” below.

Response Online

You can obtain technical support from BMC Software 24 hours a day, seven days a week by accessing the technical support Web site at **http://www.bmc.com/support.html**. From this site, you can

- read overviews about support services and programs that BMC Software offers
- find the most current information about BMC Software products
- search a database for problems similar to yours and possible solutions
- order or download product documentation
- report a problem or ask a question
- subscribe to receive e-mail notices when new product versions are released
- find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Response On Demand

In the USA and Canada, if you need technical support and do not have access to the Web, call 800 538 1872. Outside the USA and Canada, please contact your local support center or your local sales office for assistance.

Before Contacting BMC Software

Before you contact BMC Software, have the following information available so that a technical support analyst can begin working on your problem immediately:

- product information
  - product name
  - product version (release number)
  - license number and password (trial or permanent)
- operating-system and environment information
  - machine type
  - operating system type, version, and service pack or program temporary fix (PTF)
  - system hardware configuration
  - serial numbers
  - related software (database, application, and communication) including type, version, and service pack or PTF
- sequence of events leading to the problem
- commands and options that you used
- messages received (and the time and date that you received them)
  - product error messages
  - messages from the operating system, such as `file system full`
  - messages from related software

Contents

Part 1. Introduction 1

Chapter 1. MAINVIEW Products 3

Chapter 2. Introduction to MAINVIEW Security 7
Types of Security 7
Basic Security 8
Enhanced Security 8
MAINVIEW Alternate Access Security 9

Part 2. Basic Security 11

Chapter 3. Introduction to Basic Security 13
Controlling Access to Your MAINVIEW Product 13
More MAINVIEW Product Functions to Secure 13
Creating Global Security Definitions 14
Using Features of Your External Security Manager 14
What Is Required for Basic Security? 15
Phase 1: Reviewing the Resources for the Products You Want to Secure 15
Phase 2: Determining a Naming Convention 16
Phase 3: Activating Security 16

Chapter 4. Reviewing Product Resources 17
Resource Naming Convention: AutoOPERATOR, MAINVIEW for CICS, MAINVIEW for DBCTL, MAINVIEW for DB2, MAINVIEW FOCAL POINT, MAINVIEW for IMS . . . 17
Resource Naming Convention for MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR 18
Resources Used by Multiple Products 19
Resources Common to AutoOPERATOR, MAINVIEW for CICS, MAINVIEW for DB2, MAINVIEW for DBCTL, MAINVIEW for IMS, and MAINVIEW FOCAL POINT 19
Resources Common to MAINVIEW SYSPROG Services, AutoOPERATOR, and MAINVIEW for MVS 24
Resources Common to MAINVIEW for CICS and the AutoOPERATOR for CICS Option 35
Resources for AutoOPERATOR: Advanced Security 42
Resources for AutoOPERATOR Applications: (FEATURE=APPL) 44
Resources for AutoOPERATOR Commands and Transactions: (FEATURE=CMD) . . . 49
Resources for AutoOPERATOR ALERTs: (FEATURE=ALRT) 51
Resources for AutoOPERATOR EXECs: (FEATURE=EXEC) 51
Resources for AutoOPERATOR Parameter Data: (FEATURE=PARM) 52
Access through an EXCP Terminal 53
Resources for CMF MONITOR 53
Resources for MAINVIEW for CICS 54
Resources for MAINVIEW for DB2 62
Resources for MAINVIEW for DBCTL, MAINVIEW FOCAL POINT, and MAINVIEW for IMS 63
Resources for InTune 63

Chapter 5. Configuring Your ESM for Basic Security 65
Defining Security Class $BOOLE 65
Defining MAINVIEW Product Resources to Protect 66
Authorizing Access 66
Example: Securing MVS Commands for All Users 67
Example: Allowing All Users to Send Messages to the BBI-SS PAS Journal 67
Example: Allowing Mixed Accessibility 68
Identifying MAINVIEW SYSPROG Services 68
Granting or Denying Access 69
Granting Access 69
Denying Access 70
Creating Global Security Definitions: Using Generics 70
Listing MAINVIEW Product Resource Names 71

Chapter 6. Using CLISTs to Identify Resources 85
Creating Resource Names for MAINVIEW Products 86
Migrating Existing Resource Names for MAINVIEW Products 86
Creating Resource Names for AutoOPERATOR 87
Creating Resource Names for CICS Resources 88
Creating Resource Names for MAINVIEW for DB2 CMD-Level Security: DB2CMDDF and DB2CMDPE 89

Chapter 7. Activating Basic Security 91
Creating the Basic Security Member BBSEC 91
BBSEC Syntax 92
BBSEC TYPE= Statement 92
BBSEC Examples 95
Adding BBSEC to BBPARM and SYS1.PARMLIB 97
Disabling Basic Security 98

Chapter 8. Securing SYSPROG and CSMON Services 99
Activating Changes to BBSEC by Executing BBXSAF00 99
Determining the Function Qualifier for SYSPROG Resource Names 100
Using an Exit to Modify the Function Qualifier in SYSPROG Resource Names 100
Determining the Function Qualifier for CSMON Resource Names 101
Using the Password Utility 101
Password Utility JCL 102
Password Utility Return Codes 103

Part 3. Enhanced Security 105

Chapter 9. Introduction to Enhanced Security 109
Which Products Use Enhanced Security? 109
How Enhanced Security Works 110
Authorization at the CAS, PAS, and TS User Levels 110
MAINVIEW Resources 111
Resource Naming Convention 111
Finding Entity Names 113
Exploiting the Resource Naming Convention 113
Security Parameter Library 115
Sharing a Security Parameter Library Between CASs 115
Views for Administering Enhanced Security 116
Using Security Views to Change Resource Attributes 117

Establishing Enhanced Security 119
Disabling Enhanced Security for All MAINVIEW Resources 120
Determining Which Security Members Are Active 121
CAS Security Members 121
PAS Security Member 122

Chapter 10. Configuring Your ESM for Enhanced Security 123
Configuring CA-ACF2 123
Step 1: Setting the Required GSO Record Options 124
Step 2: Authorizing the PAS and CAS 124
Step 3: Updating the CA-ACF2 SAFDEF List 126
Step 4: (Optional) Adding a SAF Resource Class to CA-ACF2 127
Step 5: (Optional) Defining Rules for Controlling View Resources 129
Configuring RACF 132
Step 1: Authorizing the CAS and PAS 132
Step 2: (Optional) Adding Resource Classes to RACF 133
Step 3: Creating RACF Security Profiles 135
Step 4: Specifying Profiles to Control Access to Product Resources 136
Configuring CA-TOP SECRET 138
Step 1: Defining a New CA-TOP SECRET Facility Matrix Entry 139
Step 2: Authorizing the CAS and PAS 140
Step 3: (Optional) Adding a New SAF Resource Class 141
Step 4: Defining Ownership of Resources 142
Step 5: Controlling Access to Product Resources 143

Chapter 11. Class Definitions 145
Working with Class Definition Members 145
Displaying a List of Class Definition Members (SECDEFL) 145
Creating a Class Definition Member 146
Activating a New Class Definition Member 147
Deleting a Class Definition Member 147
Working with Class Definitions 147
Displaying a Class (SECDEF) 147
Changing a Class 149
Adding a New Class 151
Deleting a Class 152
Recovering a Deleted Class 152
Dynamically Activating Class Changes 152

Chapter 12. Parameter Definitions 155
Displaying a List of Parameter Definitions (SEPDEFL) 156
Displaying a Parameter Definition (SEPDEF and SEPDEFD) 156
Changing a Parameter Definition 157
Creating a New Parameter Definition 160
Activating a Parameter Definition 161
Deleting a Parameter Definition 161

Chapter 13. Resource Definitions 163
Before You Begin 163
Working with Resource Definition Members 164
Displaying a List of Members using the SERDEFL View 164
Creating a New Resource Definition Member 164
Activating a New Member for Common Resources 165
Activating a New Member for Product Resources 165

Deleting a Member . . . 166
Working with Resource Definitions . . . 167
Browsing a Resource Definition . . . 168
Enabling a Resource Definition . . . 169
Disabling a Resource Definition . . . 169
Changing a Resource Definition . . . 169
Canceling Resource Definition Changes . . . 171
Saving a Resource Definition . . . 171

Chapter 14. Protecting the MAINVIEW Security Interface . . . 173

Chapter 15. Resources Definitions Listed by Product . . . 175
Common MAINVIEW Resources . . . 175
Plex Manager Resources . . . 183
CMF MONITOR and MAINVIEW for OS/390 Resources . . . 193
MAINVIEW Alarm Manager Resources . . . 209
MAINVIEW for CICS Resources . . . 212
MAINVIEW for DATA ACCELERATOR Compression . . . 215
MAINVIEW for DB2 Resources . . . 217
MAINVIEW Explorer . . . 220
MAINVIEW for IMS Resources . . . 221
MAINVIEW for IP Resources . . . 225
MAINVIEW for MQSeries Resources . . . 226
MAINVIEW SYSPROG Services Resources . . . 251
MAINVIEW for UNIX System Services Resources . . . 255
MAINVIEW VistaPoint Resources . . . 259
MAINVIEW for VTAM Resources . . . 261
MAINVIEW for WebSphere Resources . . . 263

Chapter 16. Resource Definitions Listed by View . . . 265
Common Views . . . 265
Plex Manager Views . . . 266
CMF MONITOR and MAINVIEW for OS/390 Views . . . 267
MAINVIEW Alarm Manager Views . . . 275
MAINVIEW for CICS Views . . . 276
MAINVIEW for DATA ACCELERATOR Compression Views . . . 280
MAINVIEW for DB2 Views . . . 281
MAINVIEW Explorer Views . . . 282
MAINVIEW for IMS Views . . . 283
MAINVIEW for IP Views . . . 288
MAINVIEW for MQSeries Views . . . 290
MAINVIEW SYSPROG Services Views . . . 292
MAINVIEW for UNIX System Services Views . . . 293
MAINVIEW VistaPoint Views . . . 297
MAINVIEW for VTAM Views . . . 298
MAINVIEW for WebSphere Views . . . 300

Part 4. MAINVIEW Alternate Access Security . . . 303

Chapter 17. Defining Security for MAINVIEW Alternate Access . . . 305
Understanding AutoLogon Session Security Issues . . . 305
Defining Additional Security for Terminals . . . 306
Defining Additional Security for Applications . . . 307

Configuring CA-ACF2 for MAINVIEW Alternate Access 308
Customizing Class TERMINAL Access Authorization for CA-ACF2 311
Customizing Class APPL Access Authorization for CA-ACF2 311
Configuring RACF for MAINVIEW Alternate Access 313
Customizing Class TERMINAL Access Authorization for RACF 314
Customizing Class APPL Access Authorization for RACF 314
Configuring CA-TOP SECRET for MAINVIEW Alternate Access 315
Customizing Class TERMINAL Access Authorization for CA-TOP SECRET 316
Customizing Class APPL Access Authorization for CA-TOP SECRET 317

Part 5. Appendixes, Glossary, and Index 319

Appendix A. Basic Security Problem Determination 321
Before You Contact Customer Support 321
AutoOPERATOR Advanced Security 323
SYSPROG and AutoOPERATOR 324
MAINVIEW for CICS 325

Appendix B. Default Parameters for Enhanced Security 327
Default Parameter Definitions 327
Manually Creating a Parameter Definition Member 327
Understanding Parameter Definitions 328
Default Class Definitions 337
Changing and Adding Classes 337
Manually Creating a Class Definition Member 337
Understanding Class Definitions 337
Understanding the NEXT= Parameter 350
Transformation List Values for the INTENT= Parameter 351

Appendix C. Using Product Libraries 353
Parameter Libraries 357
BBPARM 357
UBBPARM 357
IMS Parameter Library (MAINVIEW for IMS, MAINVIEW for DBCTL, and AutoOPERATOR for IMS Only) 357
Sample Libraries 358
BBSAMP 358
UBBSAMP 358
Profile Libraries 359
BBPROF 359
SBBPROF 359
User BBPROF 360
Procedure Libraries (AutoOPERATOR Only) 360
BBPROC 360
UBBPROC 360
View, Screen, and View Help Distribution Libraries 361
Site Libraries 361
User Libraries 361
Shared Libraries 362
Library Concatenation 363
Link Library 363
Product Support Data Sets 363
Image and Journal Logs 364

Product Library Customization Summary 365

Glossary 369

Index 379

Figures

1. MAINVIEW Library xvii
2. BBI Architecture 4
3. Sample BBSEC Member 92
4. Sample Job for Executing BBXSAF00 99
5. Password Utility JCL 102
6. Sample Password Utility Control Statements 103
7. Sample Password Utility Output 103
8. EZSEC View 117
9. SERDEFOV View and Default Resource Definitions 117
10. SERDEFEX View and Individual Resource Definitions 118
11. Example of Source Code for the RACF ICHRRCDE Table 134
12. Example of Source Code for the RACF ICHRFR01 Table 135
13. SECDEFL View 145
14. SECDEF View 148
15. SECDEFD View 148
16. CHANGE SECURITY CLASS DEFINITION Dialog 149
17. SECURITY CLASS DEFINITION Dialog 150
18. ADD SECURITY CLASS DEFINITION Dialog 151
19. SEPDEFL View 156
20. SEPDEFD View 157
21. CHANGE SECURITY PARAMETERS Dialog 158
22. SECURITY PARAMETERS DEFINITION Dialog 159
23. SERDEFL View in Plex Manager 164
24. SERDEFOV View 167
25. SERDEFEX View 168
26. SERDEFE View 168
27. CHANGE RESOURCE AUTHORIZATION DEFINITION Dialog 170
28. SECURITY RESOURCE DEFINITION PARAMETER MEMBER Dialog 171
29. Default BBMTSS Parameter Definition Member 328
30. Partial Default BBMTSP00 Class Definition Member 338
31. Product Library Customization 354

Tables

1. Resources for AAO, CMR, DBCTL, DMR, FOCAL, and MVIMS 20
2. Resources for MAINVIEW SYSPROG Services 25
3. CICS Action Services 35
4. List of Features for AutoOPERATOR Advanced Security 42
5. AutoOPERATOR Resources: Application-Level Security 44
6. AutoOPERATOR Resources: Command-Level Security 49
7. CICS Display Services 54
8. MAINVIEW for CICS Diagnostic Services. 61
9. MAINVIEW for DB2 Resources: Command-Level Security 62
10. AutoOPERATOR Security CLISTs. 87
11. CSMON function Qualifiers 101
12. Settings for CA-ACF2 Global System Options. 124
13. Resource Definitions Common to All MAINVIEW Products 176
14. Resource Definitions for Plex Manager. 184
15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 194
16. Resource Definitions for MAINVIEW Alarm Manager 209
17. Resource Definitions for MAINVIEW for CICS 213
18. Resource Definitions for MAINVIEW for DATA ACCELERATOR Compression . . 215
19. Resource Definitions for MAINVIEW for DB2 217
20. Resource Definitions for MAINVIEW Explorer. 220
21. Resource Definitions for MAINVIEW for IMS 221
22. Resource Definitions for MAINVIEW for IP 225
23. Resource Definitions for MAINVIEW for MQSeries. 227
24. Resource Definitions for MAINVIEW SYSPROG Services - MVSPS Service Point 252
25. Resource Definitions for MAINVIEW SYSPROG Services - MVCSMON Service Point254
26. Resource Definitions for MAINVIEW for UNIX System Services 256
27. Resource Definitions for MAINVIEW VistaPoint 259
28. Resource Definitions for MAINVIEW for VTAM 261
29. Resource Definitions MAINVIEW for WebSphere. 263
30. Common Views 265
31. Plex Manager Views 266
32. CMF MONITOR and MAINVIEW for OS/390 Views. 267
33. MAINVIEW Alarm Manager Views. 275
34. MAINVIEW for CICS Views 276
35. MAINVIEW for DATA ACCELERATOR Compression Views. 280
36. MAINVIEW for DB2 Views. 281
37. MAINVIEW Explorer Views 282
38. MAINVIEW for IMS Views 283
39. MAINVIEW for IP Views. 288
40. MAINVIEW for MQSeries Views 290
41. MAINVIEW SYSPROG Services Views 292
42. MAINVIEW for UNIX System Services Views 293
43. MAINVIEW VistaPoint Views 297
44. MAINVIEW for VTAM Views. 298
45. MAINVIEW for WebSphere Views 300
46. Parameter Definitions 329
47. Class Definitions 339
48. Access Intent Interpretations by the ESM, for a Transformation 351
49. Access Intent Interpretations for Level1 351
50. MAINVIEW Product Library Configuration. 365

About This Book

This book describes how to implement MAINVIEW security with your external security manager (ESM) to protect MAINVIEW product resources from user access. It is intended for the system administrator who needs to know how to secure MAINVIEW resources.

How This Book Is Organized

Read those chapters that apply to the MAINVIEW products you intend to secure.

- **Part 1: Introduction**

  This part describes the different types of security used to secure MAINVIEW products and explains which products use which types of security.

- **Part 2: Basic Security**

  This part contains chapters that describe basic security and the steps for protecting MAINVIEW products using this type of security. To determine if your MAINVIEW product requires basic security, see “Types of Security” on page 7. For a definition of basic security, see “Basic Security” on page 8.

- **Part 3: Enhanced Security**

  This part contains chapters that describe enhanced security and the steps for protecting MAINVIEW products using this type of security. To determine if your MAINVIEW product supports enhanced security, see “Types of Security” on page 7. For a definition of enhanced security, see “Enhanced Security” on page 8.

- **Part 4: MAINVIEW Alternate Access Security**

  This part contains chapters that describe how to protect MAINVIEW Alternate Access resources.

- **Part 5: Appendixes, Glossary, and Index**

  This part contains

  – Appendix A, “Basic Security Problem Determination”
  – Appendix B, “Default Parameters for Enhanced Security”
  – Appendix C, “Using Product Libraries”
  – Glossary
  – Index

Notation Conventions

The following symbols define command syntax and should never be typed:

- Brackets [ ] enclose optional parameters or keywords.
- Braces { } enclose a list of parameters; one must be chosen.
- A line | separates alternative options; one can be chosen.
- An underlined parameter is the default.
- An ITEM IN CAPITAL LETTERS indicates exact characters; usage can be all uppercase or lowercase.
- Items in *italicized, lowercase* letters are values that you supply.
- Commands in uppercase and lowercase letters, such as HSplit, show the command abbreviation by uppercase letters (HS, for example); lowercase letters complete the entire command name as an optional entry.

  Commands that do not have an abbreviation are in all uppercase letters, such as END.

Recommended Documentation

You may want to refer to the following documentation for more product information:

For information about	**See**
CA-ACF2	*CA-ACF2 MVS Administrator Guide* *CA-ACF2 MVS General Information Guide* *CA-ACF2 MVS Systems Programmer Guide* *CA-ACF2 MVS Implementation Planning Guide*
CA-TOP SECRET	*CA-TOP SECRET MVS Planning Guide* *CA-TOP SECRET MVS Control Options Guide* *CA-TOP SECRET MVS TSS Command Functions Guide* *CA-TOP SECRET MVS Implementation: General Guide* *CA-TOP SECRET MVS Implementation: Batch and STC Guide* *CA-TOP SECRET MVS Implementation: TSO Guide* *CA-TOP SECRET MVS General Concepts Guide*
RACF	*RACF Command Language Reference* *RACF Security Administrator's Guide* *RACF General User's Guide* *RACF General Information*
VTAM	*VTAM Installation and Resource Definition* *VTAM Messages and Codes* *VTAM Operation*
MAINVIEW Alternate Access	*MAINVIEW Alternate Access Implementation and User Guide*

Related Documentation

Figure 1 shows all of the MAINVIEW books and their intended use.

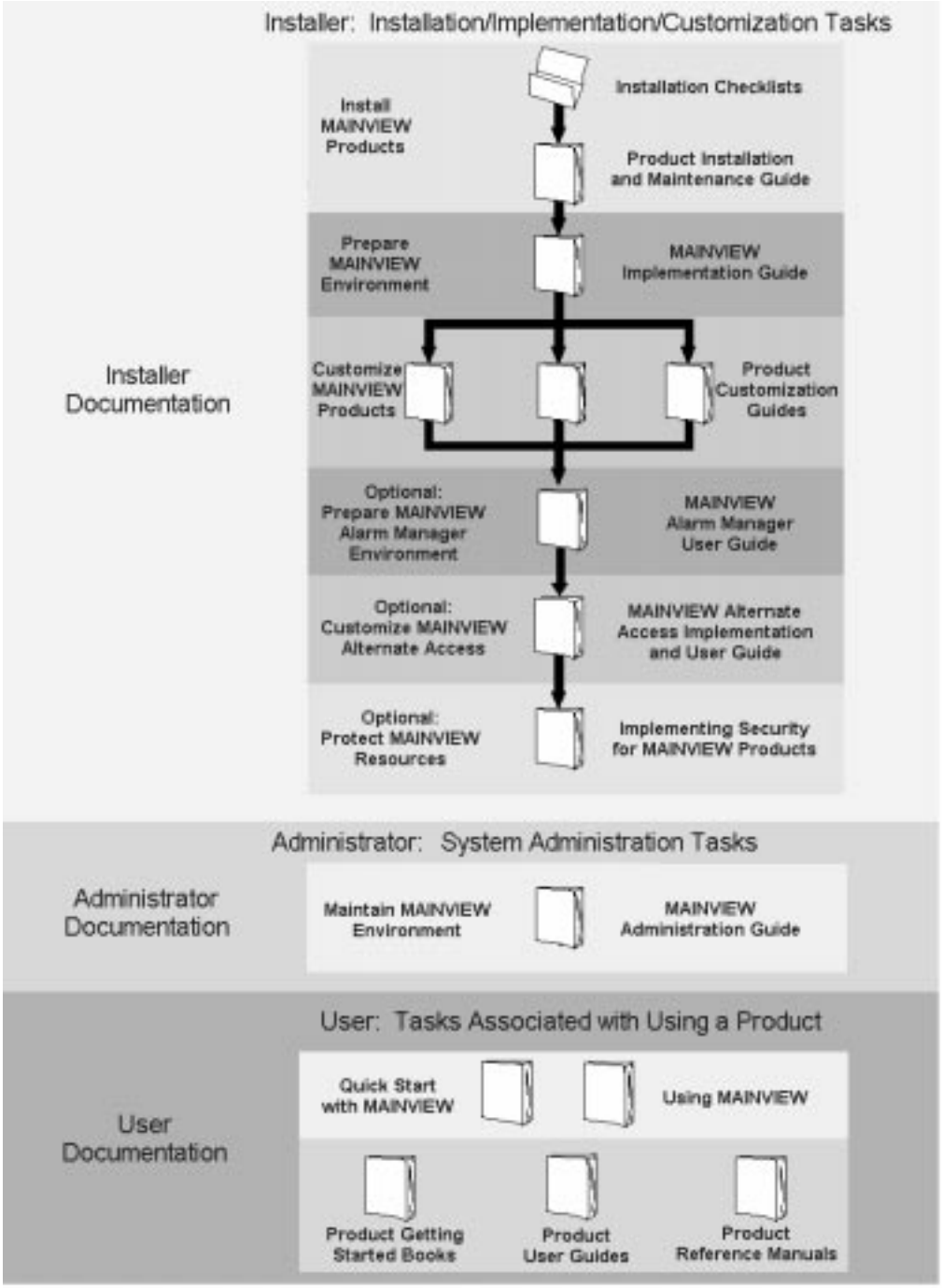


Figure 1. MAINVIEW Library

What's New

The book includes the following changes:

- The following new views are available for administering enhanced security:

  EZSEC
  EZSECRES
  SERDEFP
  SERDEFC
  SERDEFOV
  SERDEFEX

  See "Views for Administering Enhanced Security" on page 116 for more information on these views.

- RESOLVE PLUS has been renamed to MAINVIEW SYSPROG Services. This book has been updated to reflect that change. Additionally, the BBSEC member TYPE statement now supports TYPE=SYSPROG, as well as TYPE=RESOLVE.

- Command MQ for S/390 has been renamed to MAINVIEW for MQSeries. This book has been updated to reflect that change.

- Two new resource definitions for the MAINVIEW for DB2 ZP*xxxxx* views have been added.

- A new resource definition for the DIAGSTOR diagnostic view has been added.

- Information for the following products has been added to Chapter 15, "Resources Definitions Listed by Product" and Chapter 16, "Resource Definitions Listed by View":

  MAINVIEW for DATA ACCELERATOR Compression
  MAINVIEW Explorer
  MAINVIEW for IP
  MAINVIEW for VTAM
  MAINVIEW for WebSphere

- The appendix about "BMC Software Proprietary Security" contained obsolete information and has been removed from this book.

Part 1. Introduction

This part describes the different types of security used to secure MAINVIEW products.

Chapter 1. MAINVIEW Products 3

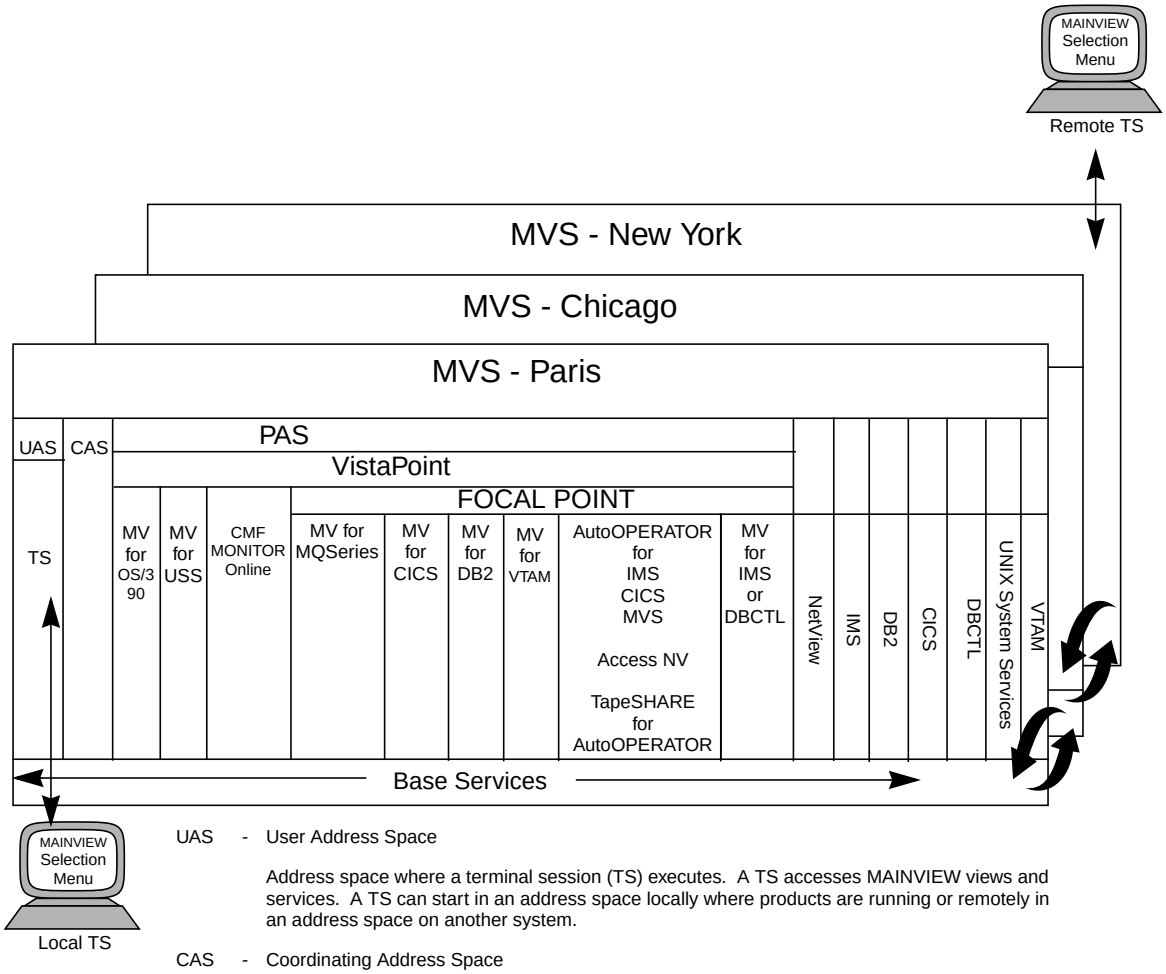
Chapter 2. Introduction to MAINVIEW Security 7
Types of Security 7
Basic Security 8
Enhanced Security 8
MAINVIEW Alternate Access Security 9

Chapter 1. MAINVIEW Products

MAINVIEW is an integrated family of performance management and automation products that monitor and control traditional and parallel mainframes. MAINVIEW comprises performance monitors, automated operations, and automation applications.

MAINVIEW product integration allows host system monitoring and automation (even in remote locations) through a common terminal session (TS), using the MAINVIEW Selection Menu. The integration of MAINVIEW products is provided through intercommunications technology known as BBI.

BBI integrates the MAINVIEW performance products within a common communications framework that operates across multiple machines in multiple locations as shown in Figure 2. This integrated architecture allows a single TS, using one or more MAINVIEW products, to monitor and manage multiple local or remote targets, whether MVS itself (sysplex and nonsysplex) or subsystems like CICS, IMS, and DB2.



UAS - User Address Space

Address space where a terminal session (TS) executes. A TS accesses MAINVIEW views and services. A TS can start in an address space locally where products are running or remotely in an address space on another system.

CAS - Coordinating Address Space

Manage communication with other local and remote CASs and enables direct communication between a TS and a PAS.

PAS - Product Address Space

Contains data collectors and runs MAINVIEW products as follows:

MVS PAS	CMF MONITOR MAINVIEW for OS/390 MAINVIEW for UNIX System Services VistaPoint for MVS workloads
BBI-SS PAS	AutoOPERATOR products MAINVIEW for: CICS DB2 DBCTL IMS MQSeries (formerly known as Command MQ for S/390) VTAM VistaPoint for CICS, DB2, and IMS workloads
MVALARM PAS	MAINVIEW Alarm Manager

Base Services - BMC Software Base Technology

Figure 2. BBI Architecture

This architecture features a built-in separation of the data, application, and end-use dimensions of systems management for maximum flexibility and extensibility. BBI communications, data collection, and the end-user terminal session (TS) execute in three distinct address spaces:

- Coordinating Address Space (CAS)
- Product Address Space (PAS)
- User Address Space (UAS)

This multiple address space structure provides a consistent, flexible environment for managing literally hundreds of MVS systems. Depending on the products installed, this allows you to

- Access different systems and products quickly and easily with simple target switching, direct hyperlinks between products, or multiple concurrent views on one TS screen
- Summarize data on a single system or across multiple MVS images
- View historical or realtime data from multiple systems summarized into one view
- Enter commands for multiple products on multiple systems
- Apply simple or complex data filtering conditions

Coordinating Address Space (CAS): The CAS runs as a subsystem and is used by most of the MAINVIEW products. It manages communication with other CASs on other local and remote sytems and allows direct communication between an individual TS and a product address space. Usually, there is one CAS per MVS system image, but there is no limit to the number of remote systems with CASs with which a single CAS can communicate.

A product establishes an independent connection with its local CAS, so you can add new products or new upgrades to the architecture without affecting existing products or other configurations.

Each CAS contains a product called Plex Manager that provides administration and operations views that help you manage communication links with other CASs, monitor the activity of accessible products, create SSI contexts, and control security for products.

Product Address Space (PAS): The PAS runs as an MVS subsystem. It comprises special routines, including data collectors, to support one or more MAINVIEW products.

- The MVS PAS services support the following MAINVIEW products:
  - CMF MONITOR
  - MAINVIEW for OS/390
  - MAINVIEW for UNIX System Services
  - MAINVIEW VistaPoint (for MVS workloads)

  There is one MVS PAS per MVS image. The MVS PAS always connects to the CAS on that MVS image.

- The BBI-SS PAS services support the following MAINVIEW products:

  – AutoOPERATOR
  – MAINVIEW for CICS
  – MAINVIEW for DB2
  – MAINVIEW for DBCTL
  – MAINVIEW for IMS
  – MAINVIEW for MQSeries (formerly known as Command MQ for S/390)
  – MAINVIEW VistaPoint (for CICS, DB2, and IMS workloads)
  – MAINVIEW for VTAM

  Multiple instances of the BBI-SS PAS can execute on a single MVS image and contain one or more products. Depending on the products installed, the BBI-SS PAS may or may not connect to a CAS on that MVS image.

  BBI-SS PASs on local and remote systems are linked together to provide cross-system communication for an individual TS through a local BBI-SS PAS to any other BBI-SS PAS.

- The MAINVIEW Alarm Manager PAS services support the following MAINVIEW products:

  – CMF MONITOR
  – MAINVIEW for CICS
  – MAINVIEW for DB2
  – MAINVIEW for IMS
  – MAINVIEW for MQSeries (formerly known as Command MQ for S/390)
  – MAINVIEW for OS/390
  – MAINVIEW for UNIX System Services
  – MAINVIEW VistaPoint

  These products must be connected to the same CAS as MAINVIEW Alarm Manager. See the *MAINVIEW Alarm Manager User Guide* for more information.

User Address Space (UAS): The UAS is the home for a terminal session (TS) connected to a 3270 terminal. A TS provides the end-user session for all MAINVIEW products. The TS connects to a CAS if there is one available or to a BBI-SS PAS or to both. There are two types of UASs:

- TSO address space

  Using a TSO address space, your TS can access MAINVIEW products and perform other TSO/ISPF functions.

- VTAM or EXCP address space using MAINVIEW Alternate Access

  Using a separate address space that communicates with your terminal with either VTAM or EXCP, your TS can access MAINVIEW products and also perform other ISPF functions.

Note: MAINVIEW Explorer provides access to MAINVIEW products from a Web browser. For more information, see the *MAINVIEW Explorer Implementation and User Guide*.

Chapter 2. Introduction to MAINVIEW Security

This chapter explains the differences between the various types of security available for MAINVIEW products.

Types of Security

There are three types of security for MAINVIEW products:

- basic security
- enhanced security
- MAINVIEW Alternate Access security

The type or types of security you implement depend on what products you have installed and how you access them.

MAINVIEW products can operate in windows mode, full-screen mode, or both. When operating in windows mode, one or more windows are displayed on your screen. When operating in full-screen mode, the product application or service is displayed on your entire screen. Some products run only in full-screen mode; some run only in windows mode; and some run in both modes.

MAINVIEW products that operate only in full-screen mode use only basic security. Products that operate only in windows mode use only enhanced security. Products that operate in both full-screen and windows mode use both basic and enhanced security.

MAINVIEW Alternate Access, which provides access to products through VTAM and EXCP interfaces without an active TSO subsystem, requires its own security. Security for MAINVIEW Alternate Access is independent of basic or enhanced product security.

Products That Use Only Basic Security

The following products operate only in full-screen mode and use only basic security:

AutoOPERATOR
MAINVIEW FOCAL POINT

Products That Use Only Enhanced Security

The following products operate only in windows mode and use only enhanced security:

CMF Monitor Online
MAINVIEW Alarm Manager
MAINVIEW for DATA ACCELERATOR Compression
MAINVIEW Explorer
MAINVIEW for IP
MAINVIEW for MQSeries (formerly known as Command MQ for S/390)
MAINVIEW for OS/390
MAINVIEW for UNIX System Services
MAINVIEW VistaPoint

MAINVIEW for VTAM
MAINVIEW for WebSphere

Products That Use Basic and Enhanced Security

The following products operate in both full-screen and windows mode and use both basic and enhanced security:

MAINVIEW for CICS
MAINVIEW for DBCTL
MAINVIEW for DB2
MAINVIEW for IMS
MAINVIEW SYSPROG Services

Basic Security

The three types of security have different characteristics. Basic security

- uses the standard MVS SAF RACROUTE AUTH calls to communicate with your external security manager
- supports RACF, CA-ACF2, and CA-Top Secret
- uses the security class name $BOOLE by default; however, you can use any security class
- uses fixed, predefined resource names to identify MAINVIEW resources
- requires that you define resources to your ESM and grant or deny access to them
- is administered outside of MAINVIEW using the BBSEC member in SYS1.PARMLIB

To implement basic security, see "Introduction to Basic Security" on page 13.

Enhanced Security

Unlike basic security, enhanced security

- uses the standard MVS SAF interface to communicate with your external security manager
- supports RACF, CA-ACF2, CA-Top Secret, or any SAF-compliant security interface
- fulfills the requirements for United States Department of Defense B1 security
- uses the security class name FACILITY by default; however, you can use any security class
- uses customizes resource names to identify MAINVIEW resources
- requires that you define resources to your ESM and grant or deny access to them
- is administered through MAINVIEW security views (EZSEC, EZSECRES, SECDEF, SEPDEF, SERDEF, SERDEFP, SERDEPC, SERDEFOV, and SERDEFEX)
- stores security definition members in a security parameter library

This library is referenced by the BBSECURE DD statement in the CAS and PAS started task procedures. The members in the library are read during CAS and PAS initialization to establish security.

- provides group resource definitions

  Resources included in a group definition inherit the security characteristics of that group, making it easy to define one resource definition that effects dozens or hundreds—even thousands— of resources. The security characteristics of individual resources in a group resource definition can be further defined as needed.

To implement enhanced security, see "Introduction to Enhanced Security" on page 109.

MAINVIEW Alternate Access Security

MAINVIEW Alternate Access provides VTAM and EXCP interfaces to ISPF for accessing MAINVIEW products, without requiring an active TSO subsystem. MAINVIEW Alternate Access uses the standard MVS SAF interface to communicate with your external security manager (ESM) and requires that each user ID for a session be defined to your ESM.

To implement MAINVIEW Alternate Access security, see Chapter 17, "Defining Security for MAINVIEW Alternate Access" on page 305.

Note: MAINVIEW Alternate Access security is independent of basic or enhanced product security. The information in this book related to basic and enhanced security does not apply to MAINVIEW Alternate Access.

Part 2. Basic Security

This part describes basic security and the steps users of MAINVIEW products requiring basic security should take to secure their products.

Chapter 3. Introduction to Basic Security 13
Controlling Access to Your MAINVIEW Product 13
More MAINVIEW Product Functions to Secure 13
Creating Global Security Definitions 14
Using Features of Your External Security Manager 14
What Is Required for Basic Security? 15
Phase 1: Reviewing the Resources for the Products You Want to Secure 15
Phase 2: Determining a Naming Convention 16
Phase 3: Activating Security 16

Chapter 4. Reviewing Product Resources 17
Resource Naming Convention: AutoOPERATOR, MAINVIEW for CICS, MAINVIEW for DBCTL, MAINVIEW for DB2, MAINVIEW FOCAL POINT, MAINVIEW for IMS . . . 17
Resource Naming Convention for MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR 18
Resources Used by Multiple Products 19
Resources Common to AutoOPERATOR, MAINVIEW for CICS, MAINVIEW for DB2, MAINVIEW for DBCTL, MAINVIEW for IMS, and MAINVIEW FOCAL POINT 19
Resources Common to MAINVIEW SYSPROG Services, AutoOPERATOR, and MAINVIEW for MVS 24
Resources Common to MAINVIEW for CICS and the AutoOPERATOR for CICS Option 35
Resources for AutoOPERATOR: Advanced Security 42
Resources for AutoOPERATOR Applications: (FEATURE=APPL) 44
Resources for AutoOPERATOR Commands and Transactions: (FEATURE=CMD) . . . 49
Resources for AutoOPERATOR ALERTs: (FEATURE=ALRT) 51
Resources for AutoOPERATOR EXECs: (FEATURE=EXEC) 51
Resources for AutoOPERATOR Parameter Data: (FEATURE=PARM) 52
Access through an EXCP Terminal 53
Resources for CMF MONITOR 53
Resources for MAINVIEW for CICS 54
Resources for MAINVIEW for DB2 62
Resources for MAINVIEW for DBCTL, MAINVIEW FOCAL POINT, and MAINVIEW for IMS 63
Resources for InTune 63

Chapter 5. Configuring Your ESM for Basic Security 65
Defining Security Class $BOOLE 65
Defining MAINVIEW Product Resources to Protect 66
Authorizing Access 66
Example: Securing MVS Commands for All Users 67
Example: Allowing All Users to Send Messages to the BBI-SS PAS Journal 67
Example: Allowing Mixed Accessibility 68
Identifying MAINVIEW SYSPROG Services 68
Granting or Denying Access 69
Granting Access 69
Denying Access 70
Creating Global Security Definitions: Using Generics 70

Listing MAINVIEW Product Resource Names 71

Chapter 6. Using CLISTs to Identify Resources 85
Creating Resource Names for MAINVIEW Products. 86
Migrating Existing Resource Names for MAINVIEW Products 86
Creating Resource Names for AutoOPERATOR 87
Creating Resource Names for CICS Resources 88
Creating Resource Names for MAINVIEW for DB2 CMD-Level Security: DB2CMDDF and DB2CMDPE 89

Chapter 7. Activating Basic Security 91
Creating the Basic Security Member BBSEC 91
BBSEC Syntax 92
BBSEC TYPE= Statement 92
BBSEC Examples. 95
Adding BBSEC to BBPARM and SYS1.PARMLIB 97
Disabling Basic Security 98

Chapter 8. Securing SYSPROG and CSMON Services 99
Activating Changes to BBSEC by Executing BBXSAF00 99
Determining the Function Qualifier for SYSPROG Resource Names 100
Using an Exit to Modify the Function Qualifier in SYSPROG Resource Names. 100
Determining the Function Qualifier for CSMON Resource Names 101
Using the Password Utility 101
Password Utility JCL 102
Password Utility Return Codes. 103

Chapter 3. Introduction to Basic Security

This chapter describes how to plan for and implement security with your external security manager (ESM) for the following MAINVIEW products and components:

- AutoOPERATOR
- MAINVIEW for CICS
- MAINVIEW for DBCTL
- MAINVIEW for DB2
- MAINVIEW FOCAL POINT
- MAINVIEW for IMS
- MAINVIEW SYSPROG Services and Common Storage Monitor

The remainder of this chapter describes implementing basic security for your MAINVIEW products using RACF as the ESM.

Note: The information in this chapter does not apply to MAINVIEW Alternate Access. To implement MAINVIEW Alternate Access security, see "Defining Security for MAINVIEW Alternate Access" on page 305.

Controlling Access to Your MAINVIEW Product

Using basic security enables you to specify

- which actions or commands can be performed
- which data is available to view
- on which BBI-SS PAS the feature can be accessed or the action performed
- on which targets the feature can be accessed or the action performed

For example, a resource might be an action such as accessing a certain application or issuing MVS commands. To secure a user's ability to issue MVS commands, you can specify

- which user IDs can issue MVS commands
- in which BBI-SS PAS MVS commands can be invoked
- to which targets MVS commands can be directed

Some MAINVIEW products allow you to secure many resources. Determining how you want to secure these resources requires careful planning. Refer to Chapter 4, "Reviewing Product Resources" on page 17 for more information about what you can secure.

More MAINVIEW Product Functions to Secure

Many MAINVIEW products allow you to create security for more of the products' functions than was previously possible with BMC Software proprietary security. For example, in AutoOPERATOR Version 3.1.0, you can implement advanced security features that allow you to secure who can access specific AutoOPERATOR applications, issue commands, and even who can schedule individual EXECs by EXEC name.

Potentially, added security might mean more work and planning. As an example, if you decide to implement the advanced security feature in AutoOPERATOR that secures EXECs by EXEC

name, you will have to review all the EXECs in your library and then decide which user ID will have access to which EXECs, on which BBI-SS PASs.

For more information, refer to the sections in Chapter 4, “Reviewing Product Resources” on page 17, that describe the functions of a product you can secure.

Creating Global Security Definitions

If your ESM supports using generics and your security scheme allows it, securing MAINVIEW products through the ESM will allow you to use generics in naming MAINVIEW product resources to create global security definitions. This can be accomplished by defining an entire set of resources that will be available either to a select group of users or to all users. For example, you may allow all users to display applications, but only a subset of users to update them.

You can identify a group of users who will have access to all areas of a product. For example, system administrators may need to be to able perform all functions in all areas, but operators can perform their jobs without needing access to all areas. Creating global security definitions can make this process simpler to perform.

Refer to “Creating Global Security Definitions: Using Generics” on page 70 for information about using generics for your security system.

Using Features of Your External Security Manager

You might also consider how to best use security features offered by your ESM. For example, your ESM may offer auditing functions that you can turn on to track the usage of resources. In instances where security is a high priority, messages that record violation attempts can be routed to a line terminal or console for immediate notification. Refer to your ESM documentation for information on the various security features offered.

What Is Required for Basic Security?

Implementing basic security for the AutoOPERATOR, Mainview for CICS, MAINVIEW for DB2, MAINVIEW for DBCTL, MAINVIEW FOCAL POINT, MAINVIEW for IMS, and MAINVIEW SYSPROG Services is a three-phase process:

- In the first phase, begin by examining the resources available within each product. A resource is anything you can protect, and includes such things as opening a database or executing a command.

  Note that security for these products is accomplished on a subsystem (BBI-SS PAS) by subsystem basis. Therefore, you may decide that one BBI-SS PAS warrants more security than another; for example, a test BBI-SS PAS may have less security requirements than a production BBI-SS PAS.

  In addition, some products provide greater control over how the product is secured and what can be secured. Become familiar with your product so you can determine the most beneficial security to implement for your site.

- Once you have determined what to secure, the second phase consists of learning how resources are named and defined.

  Creating names for BBI-SS PAS product resources allows you to specify for which targets the resources are secured.

  The first two phases require mostly planning and examining how a MAINVIEW product needs to be secured at your site. Once these phases are complete, the third phase is relatively simple to complete.

- The third phase involves creating a security class in the ESM to identify the resources to the ESM, grant or deny access to a resource, and turn security on.

The following sections provide a brief overview of the tasks you need to complete to implement basic security with your ESM.

Phase 1: Reviewing the Resources for the Products You Want to Secure

Regardless of which MAINVIEW products (or how many) you are implementing security for, your first task should be to review the resources for each product you are going to secure.

Some resources, once secured for one product, are secured for other products as well. For example, if you secure certain resources for AutoOPERATOR, these resources are also secured for MAINVIEW for CICS, MAINVIEW for DB2, MAINVIEW for IMS, and so on.

The resources available for security are listed by each product, in alphabetical order in Chapter 4, “Reviewing Product Resources”. To aid you, “Listing MAINVIEW Product Resource Names” on page 71 provides a matrix, listing each resource and which products use it. This way, you can establish easily how securing a specific resource for one product might affect your other products.

Phase 2: Determining a Naming Convention

This step requires that you plan your security for products on a BBI-SS PAS by BBI-SS PAS basis. The subsystem name is part of the resource name and determines the BBI-SS PAS for which the particular resource is secured.

For example, you may decide to limit users that have update access to the AutoOPERATOR Rules Processor application on your production BBI-SS PAS, but allow everyone to have update access on your test BBI-SS PAS. In this case, you would have two resource names, one for each BBI-SS PAS. Each of these resource names must be identified to the ESM so you can begin specifying who or what group of users can access each resource.

Chapter 4, “Reviewing Product Resources” on page 17, has complete information about naming conventions and how they affect your security scheme.

Users of products that require enhanced security may also want to adapt a convention compatible with both basic and enhanced security.

Phase 3: Activating Security

Once you have determined which resources to secure and understand how to use the naming convention, you need to

- create a security class in the ESM for your MAINVIEW products
- identify the fully named resources to the ESM
- grant or deny access to the resources
- turn on security

Chapter 6, “Using CLISTs to Identify Resources” on page 85 explains how use BMC Software-supplied CLISTs to help you with naming your resources. Chapter 7, “Activating Basic Security” on page 91 explains how to activate security.

Chapter 4. Reviewing Product Resources

This chapter explains the naming convention for resource names and lists all the resources, alphabetically by product, that you can secure through the ESM installed at your site.

Resource Naming Convention: AutoOPERATOR, MAINVIEW for CICS, MAINVIEW for DBCTL, MAINVIEW for DB2, MAINVIEW FOCAL POINT, MAINVIEW for IMS

Resource names for the following products:

AutoOPERATOR
MAINVIEW for CICS
MAINVIEW for DBCTL
MAINVIEW for DB2
MAINVIEW FOCAL POINT
MAINVIEW for IMS

are defined on a BBI-SS PAS by BBI-SS PAS basis. The subsystem name is part of the resource name and determines the BBI-SS PAS for which the resource is secured. You must specify the BBI-SS PAS and target when defining a resource to your ESM.

The resource naming convention for these products is

prefix.ssid.product.target.suffix

When creating permits, profiles, and rules to control access to resources, an explicit or generic value can be specified for any qualifier in the resource name by using the masking characters supported by the ESM. For example, an explicit resource name might look like this:

```
BBM.BBCS.AAO.TARGET01.RULEREAD
```

A generic resource name with a RACF wildcard (*) used in the *ssid* qualifier might look like this:

```
BBM.BB*.CICS.TARGET02.CONNECT.SESSIONS
```

The resource name qualifiers are as follows:

prefix — The 1- to 8-character prefix used for all resource names. If you do not specify a prefix, the default prefix is BBM, which is added automatically to all resource names.

ssid — The 1- to 4-character subsystem ID of the BBI-SS PAS for which the resource is to be secured. The SSIDs are specified in BBPARM member BBIJNT00. You must include the SSID in the resource name.

product One of the following product abbreviations:

BBI	Common resources
AAO	AutoOPERATOR resources
CMR	MAINVIEW for CICS resources
DBCTL	MAINVIEW for DBCTL resources
DMR	MAINVIEW for DB2 resources
FOCAL	MAINVIEW FOCAL POINT resources
MVIMS	MAINVIEW for IMS resources

target The 1- to 8-character target name (as displayed in the right corner of a MAINVIEW session panel) that specifies to which target the action is directed. All valid target names are listed in BBPARM member BBIJNT00. You must include the target name in the resource name.

suffix A predefined suffix that represents the actual function the resource represents. The remainder of this chapter lists the resource names, including the suffix for each resource. The suffix can consist of a BMC Software-supplied portion and a user-specified portion.

Resource Naming Convention for MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR

The resource naming convention for MAINVIEW SYSPROG Services and COMMON STORAGE MONTIOR services is

prefix.sysid.product.service.function

When creating permits, profiles, and rules to control access to resources, an explicit or generic value can be specified for any qualifier in the resource name by using the masking characters supported by the ESM. For example, an explicit resource name might look like this:

```
BBM.SYSA.RESOLVE.AUTHTSO.LIST
```

A generic resource name with a RACF wildcard (*) used in the *sysid* qualifier might look like this:

```
BBM.SYS*.RESOLVE.DEALLOC.UPDATE
```

The resource name qualifiers are as follows:

prefix The 1- to 8-character prefix used for all resource names. The default prefix is BBM, which is appended to all resource names.

sysid The SYSNAME (or SMFID) of the system where the service is to be executed.

product The name of the product issuing the request (RESOLVE for MAINVIEW SYSPROG Services or CSMON for COMMON STORAGE MONITOR).

service The name of the service to be executed.

function One of the following values:

LIST	for services that display information
UPDATE	for services that update system resources
user-defined	For MAINVIEW SYSPROG Services, the function qualifier can be modified by a user exit as described on page 100.

Some services perform either a list or an update function depending on the service operands specified by the user. Table 2 on page 25 lists the resource name or names for each service.

You may want to consider denying access to all requests with a function qualifier of UPDATE. You can then make exceptions for specific users or groups of users on a service-by-service basis.

Resources Used by Multiple Products

Some BMC Software products share resources. For example, if you have MAINVIEW for CICS and the AutoOPERATOR for CICS option, securing MAINVIEW for CICS resources also secures those same resources in AutoOPERATOR.

The sections below describe which resources affect multiple products.

Resources Common to AutoOPERATOR, MAINVIEW for CICS, MAINVIEW for DB2, MAINVIEW for DBCTL, MAINVIEW for IMS, and MAINVIEW FOCAL POINT

If you have any of the following products, or a combination of these products, use the information in this section to determine how securing a resource in one product might affect another product:

Product	Abbreviation
AutoOPERATOR	AAO
MAINVIEW for CICS	CMR
MAINVIEW for DBCTL	DBCTL
MAINVIEW for DB2	DMR
MAINVIEW FOCAL POINT	FOCAL
MAINVIEW for IMS	MVIMS
Common resources	BBI

Not all resources are applicable to all products, so the third column in the following table lists which products use this resource.

If you plan to implement security for any of these products, the resources listed in this table must be secured before you can implement security within each individual product.

For an explanation of the resource naming convention used in this table, see page 17.

Table 1. Resources for AAO, CMR, DBCTL, DMR, FOCAL, and MVIMS

To protect this resource	Use this resource name	Affects products
Accessing a BBI target	Accessing a specific target or targets. **Resource Name:** *prefix.ssid*.BBI.target.ACCESS **Note:** Securing this resource is a prerequisite to implementing security for any other resource in this table. Access to the BBI-SS PAS (or target) is always checked before access to a specific product resource is checked.	AAO CMR DBCTL DMR MVIMS FOCAL
Issuing BBI control commands	Issuing BBI control commands such as .RESET, .CANCEL, .STOP, .START. **Resource Name:** *prefix.ssid*.BBI.target.BBICMD	AAO CMR DBCTL DMR MVIMS
Writing messages to the BBI Journal log	Writing messages to BBI Journal log. **Resource Name:** *prefix.ssid*.BBI.target.JRNLMSG	AAO CMR DBCTL DMR MVIMS
Dynamic data set allocation of trace log data sets	Granting access to this resource allows the BBI-SS PAS to allocate trace log data sets dynamically for this user. Denying access specifies that the BBI-SS PAS is not to allocate the trace log data sets. Trace logging can be requested only if trace log data sets are preallocated. If access is denied and a trace log data set does not exist, a request for trace logging will fail. **Note:** Only a DISPOSITION of OLD is accepted for trace log data set allocation if access is denied. **Resource Name:** *prefix.ssid*.BBI.target.TRALLOC	CMR DMR MVIMS DBCTL
Starting a summary application trace	Starting a summary trace (accounting). **Resource Name:** *prefix.ssid*.BBI.target.TRACE.S	CMR DBCTL DMR MVIMS
Starting a summary or detail application trace	Starting a summary trace plus detail trace with SQL events. **Resource Name:** *prefix.ssid*.BBI.target.TRACE.D	CMR DBCTL DMR MVIMS

Table 1. Resources for AAO, CMR, DBCTL, DMR, FOCAL, and MVIMS (Continued)

To protect this resource	Use this resource name	Affects products
Starting a summary or detail application trace (with all events for MAINVIEW for DB2)	Starting a detail trace plus scans, I/Os, locks, and DDF detail event tracing. **Resource Name:** *prefix.ssid.*BBI.target.TRACE.ALL TRACE.ALL supersedes TRACE.S or TRACE.D.	DMR CMR MVIMS
Issuing MVS commands	Issuing MVS commands such as VARY, START, STOP, CANCEL. **Resource Name:** *prefix.ssid.*AAO.target.MVSCMD	AAO
Displaying the AutoOPERATOR Rules Processor application	Accessing and displaying the Rules within the Rules Processor. Users with display-only access cannot perform any actions that would affect automation. **Resource Name:** *prefix.ssid.*AAO.target.RULEREAD This resource is a prerequisite to implementing AutoOPERATOR advanced security. For more information, refer to "Resources for AutoOPERATOR: Advanced Security" on page 42.	AAO
Updating the AutoOPERATOR Rules Processor application	Updating and creating new Rules in the Rules Processor application. Users with update access can take actions that effect automation, enable or disable Rule Sets, move Rules within a Rule Set, change Rule Set search strategy, and so on. **Resource Name:** *prefix.ssid.*AAO.target.RULEUPD This resource is a prerequisite to implementing AutoOPERATOR advanced security. For more information, refer to "Resources for AutoOPERATOR: Advanced Security" on page 42.	AAO
Invoking CICS transactions from an AutoOPERATOR terminal session	Invoking CICS transactions from AutoOPERATOR terminal sessions. **Resource Name:** *prefix.ssid.*AAO.target.CICSTRAN	AAO
Invoking AutoOPERATOR EXECs	Invoking AutoOPERATOR EXECs. **Resource Name:** *prefix.ssid.*AAO.target.EXEC This resource allows you to control who has authority to invoke or test EXECs. You may want to grant authority for users to have EXEC access on a test system but not on a production system. This resource is a prerequisite to implementing AutoOPERATOR advanced security. For more information, refer to "Resources for AutoOPERATOR: Advanced Security" on page 42.	AAO

Table 1. Resources for AAO, CMR, DBCTL, DMR, FOCAL, and MVIMS (Continued)

To protect this resource	Use this resource name	Affects products
Displaying AutoOPERATOR parameter data in the AutoOPERATOR Dynamic Parameter Manager	Displaying AutoOPERATOR parameter data in the AutoOPERATOR Dynamic Parameter Manager application without the authority to update it. **Resource Name:** *prefix.ssid*.AAO.target.PARMREAD This resource is a prerequisite to implementing AutoOPERATOR advanced security. For more information, refer to "Resources for AutoOPERATOR: Advanced Security" on page 42.	AAO
Updating AutoOPERATOR parameter data in the AutoOPERATOR Dynamic Parameter Manager	Updating AutoOPERATOR parameter data in the AutoOPERATOR Dynamic Parameter Manager application. **Resource Name:** *prefix.ssid*.AAO.target.PARMUPD This resource is a prerequisite to implementing AutoOPERATOR advanced security. For more information, refer to "Resources for AutoOPERATOR: Advanced Security" on page 42.	AAO
Invoking IMS transactions from an AutoOPERATOR terminal session	**Resource Name:** *prefix.ssid*.AAO.target.IMSTRAN	AAO
Invoking IMS commands from an AutoOPERATOR terminal session	**Resource Name:** *prefix.ssid*.AAO.target.IMSCMD	AAO
Sending messages to the IMS terminal	**Resource Name:** *prefix.ssid*.AAO.target.IMSMSG	AAO
Displaying AutoOPERATOR parameter data in the TapeSHARE for AutoOPERATOR Application	**Resource Name:** *prefix.ssid*.AAO.target.APPL.TAPSREAD	AAO
Updating AutoOPERATOR parameter data in the TapeSHARE for AutoOPERATOR application	**Resource Name:** *prefix.ssid*.AAO.target.APPL.TAPSUPD	AAO
Invoking SYSPROG services from an AutoOPERATOR terminal session	For additional information about securing SYSPROG services from AutoOPERATOR, refer to "Resources for AutoOPERATOR EXECs: (FEATURE=EXEC)" on page 51. **Resource Name:** *prefix.ssid*.AAO.target.RESAUTH	SYSPROG from AAO
Issuing DB2 commands in DMR	**Resource Name:** *prefix.ssid*.DMR.target.DB2CMD	DMR

Table 1. Resources for AAO, CMR, DBCTL, DMR, FOCAL, and MVIMS (Continued)

To protect this resource	Use this resource name	Affects products
Starting a DB2 application trace for the total workload (DB2AUTH = +)	**Resource Name:** *prefix.ssid*.DMR.target.DB2TRACE.GENERIC	DMR
Displaying SQL text when the ID of the event being traced matches the user ID	Specifies which SQL text can be viewed by the user with the DUSER service and the pop-up display for the BIND-TXT entry in the DTRAC service. A message is produced in place of the SQL text to inform the user that the text display was suppressed by user authorization. Granting access to this resource allows you to display only SQL text if the authorization ID of the event being traced matches the user ID connected to MAINVIEW for DB2. **Resource Name:** *prefix.ssid*.DMR.target.DB2SQLAU	DMR
Displaying all SQL text	Granting access to this resource allows you to display all SQL text. **Resource Name:** *prefix.ssid*.DMR.target.DB2SQLAL	DMR

Resources Common to MAINVIEW SYSPROG Services, AutoOPERATOR, and MAINVIEW for MVS

Table 2 lists all the services you can secure if you have access to MAINVIEW SYSPROG Services services from

- MAINVIEW SYSPROG Services as a stand-alone product
- AutoOPERATOR for MVS option of AutoOPERATOR, which includes some MAINVIEW SYSPROG Services
- MAINVIEW for MVS

The third column of Table 2 shows that securing a MAINVIEW SYSPROG Services service also secures that service if you are accessing it from the AutoOPERATOR for MVS option or from MAINVIEW for MVS.

The AutoOPERATOR for MVS option is distributed with a subset of MAINVIEW SYSPROG Services. **If you have the AutoOPERATOR for MVS option and you also have MAINVIEW SYSPROG Services**, you have the option to allow access to the full MAINVIEW SYSPROG Services product from AutoOPERATOR. When you choose this option, all the services listed in this table can be accessed from AutoOPERATOR and any existing MAINVIEW SYSPROG Services security restrictions apply. Refer to Chapter 14, “Accessing Full RESOLVE from AutoOPERATOR” in the *AutoOPERATOR Customization Guide* for more information.

All of the MAINVIEW SYSPROG services are defined in the service name table, which is distributed as member ASTXA1SN in the BBSRC data set. You can use the service name table to review or override the default *function* qualifier used in the resource name for each service. See page 100 for more information on ASTXA1SN.

Notes:

- In Table 2, MAINVIEW SYSPROG Services has been abbreviated to SYSPROG and MAINVIEW for MVS has been abbreviated to MVMVS.
- For an explanation of the resource naming convention used in Table 2, see page 18.
- You may code a user exit to modify the function qualifier for any service, as described on page 100. A default exit is provided for those services marked with an asterisk (*) in Table 2.

Table 2. Resources for MAINVIEW SYSPROG Services

Service	Resource name	Affects products
ALLOCATE	*prefix.sysid*.RESOLVE.ALLOCATE.UPDATE	SYSPROG SYSPROG from MVMVS
APF*	*prefix.sysid*.RESOLVE.APF.LIST *prefix.sysid*.RESOLVE.APF.UPDATE	SYSPROG SYSPROG from MVMVS
ASM	*prefix.sysid*.RESOLVE.ASM.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
ASVT	*prefix.sysid*.RESOLVE.ASVT.LIST	SYSPROG
AUTHTSO	*prefix.sysid*.RESOLVE.AUTHTSO.LIST *prefix.sysid*.RESOLVE.AUTHTSO.UPDATE	SYSPROG SYSPROG from MVMVS
BBXS	*prefix.sysid*.RESOLVE.BBXS.LIST	SYSPROG SYSPROG from MVMVS
CDE	*prefix.sysid*.RESOLVE.CDE.LIST	SYSPROG SYSPROG from MVMVS
CHAP	*prefix.sysid*.RESOLVE.CHAP.UPDATE	SYSPROG SYSPROG from MVMVS
CLEAR (Alias: CLR)	*prefix.sysid*.RESOLVE.CLEAR.UPDATE	SYSPROG SYSPROG from MVMVS
CNSL	*prefix.sysid*.RESOLVE.CNSL.UPDATE	SYSPROG
CONSOLES	*prefix.sysid*.RESOLVE.CONSOLES.LIST	SYSPROG SYSPROG from MVMVS
CPU	*prefix.sysid*.RESOLVE.CPU.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
CSA	*prefix.sysid*.RESOLVE.CSA.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
CSMON*	*prefix.sysid*.RESOLVE.CSMON.LIST *prefix.sysid*.RESOLVE.CSMON.UPDATE	SYSPROG SYSPROG from MVMVS
CSSUM	*prefix.sysid*.RESOLVE.CSSUM.LIST	SYSPROG SYSPROG from MVMVS
DCPU	*prefix.sysid*.RESOLVE.DCPU.LIST	SYSPROG SYSPROG from MVMVS
DEALLOC	*prefix.sysid*.RESOLVE.DEALLOC.UPDATE	SYSPROG SYSPROG from MVMVS
DEBUG	*prefix.sysid*.RESOLVE.DEBUG.UPDATE	SYSPROG
DEVIATN	*prefix.sysid*.RESOLVE.DEVIATN.LIST	SYSPROG SYSPROG from MVMVS
DOMAIN	*prefix.sysid*.RESOLVE.DOMAIN.LIST	SYSPROG SYSPROG from MVMVS
DONTSWAP	*prefix.sysid*.RESOLVE.DONTSWAP.UPDATE	SYSPROG SYSPROG from MVMVS
DSNAME	*prefix.sysid*.RESOLVE.DSNAME.LIST	SYSPROG SYSPROG from MVMVS
DUMP (Alias: LIST)	*prefix.sysid*.RESOLVE.DUMP.LIST	SYSPROG from MVMVS
DVIEW	*prefix.sysid*.RESOLVE.DVIEW.LIST	SYSPROG SYSPROG from MVMVS
DVIEW	*prefix.sysid*.RESOLVE.DVIEW.UPDATE	SYSPROG SYSPROG from MVMVS
EDTINFO	*prefix.sysid*.RESOLVE.EDTINFO.LIST	SYSPROG SYSPROG from MVMVS
ENQUEUES	*prefix.sysid*.RESOLVE.ENQUEUES.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
EQUATE	*prefix.sysid*.RESOLVE.EQUATE.LIST	SYSPROG SYSPROG from MVMVS
ESCLASS	*prefix.sysid*.RESOLVE.ESCLASS.LIST *prefix.sysid*.RESOLVE.ESCLASS.UPDATE	SYSPROG SYSPROG from MVMVS
ESTORAGE	*prefix.sysid*.RESOLVE.ESTORAGE.LIST	SYSPROG SYSPROG from AAO
EXECUTE	*prefix.sysid*.RESOLVE.EXECUTE.UPDATE	SYSPROG SYSPROG from MVMVS
EXIT	*prefix.sysid*.RESOLVE.EXIT.UPDATE	SYSPROG SYSPROG from MVMVS
FCOMMON	*prefix.sysid*.RESOLVE.FCOMMON.UPDATE	SYSPROG
FINDMBR	*prefix.sysid*.RESOLVE.FINDMBR.LIST	SYSPROG SYSPROG from MVMVS
HELP	*prefix.sysid*.RESOLVE.HELP.LIST	SYSPROG
INFO	*prefix.sysid*.RESOLVE.INFO.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
IO	*prefix.sysid*.RESOLVE.IO.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
IPLDATA	*prefix.sysid*.RESOLVE.IPLDATA.LIST	SYSPROG
LABEL	*prefix.sysid*.RESOLVE.LABEL.LIST	SYSPROG SYSPROG from MVMVS
LCPU*	*prefix.sysid*.RESOLVE.LCPU.LIST *prefix.sysid*.RESOLVE.LCPU.UPDATE	SYSPROG SYSPROG from MVMVS
LLIST*	*prefix.sysid*.RESOLVE.LLIST.LIST *prefix.sysid*.RESOLVE.LLIST.UPDATE	SYSPROG SYSPROG from MVMVS

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
LNKLST*	*prefix.sysid*.RESOLVE.LNKLST.LIST *prefix.sysid*.RESOLVE.LNKLST.UPDATE	SYSPROG SYSPROG from MVMVS
LOADLPA*	*prefix.sysid*.RESOLVE.LOADLPA.LIST *prefix.sysid*.RESOLVE.LOADLPA.UPDATE	SYSPROG SYSPROG from MVMVS
LOCKS	*prefix.sysid*.RESOLVE.LOCKS.LIST	SYSPROG SYSPROG from MVMVS
LOGGING	*prefix.sysid*.RESOLVE.LOGGING.LIST	SYSPROG
LPA	*prefix.sysid*.RESOLVE.LPA.LIST	SYSPROG SYSPROG from MVMVS
LWAIT*	*prefix.sysid*.RESOLVE.LWAIT.LIST *prefix.sysid*.RESOLVE.LWAIT.UPDATE	SYSPROG SYSPROG from MVMVS
MCOMMAND (Aliases: COMMAND, CMD and MCMD)	*prefix.sysid*.RESOLVE.MCOMMAND.UPDATE	SYSPROG SYSPROG from MVMVS
MDEVICE	*prefix.sysid*.RESOLVE.MDEVICE.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
MEMSCAN	*prefix.sysid*.RESOLVE.MEMSCAN.LIST	SYSPROG SYSPROG from MVMVS
MIO	*prefix.sysid*.RESOLVE.MIO.LIST	SYSPROG SYSPROG from MVMVS
MLCU	*prefix.sysid*.RESOLVE.MLCU.LIST	SYSPROG SYSPROG from MVMVS
MONITOR	*prefix.sysid*.RESOLVE.MONITOR.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
MOUNT	*prefix.sysid*.RESOLVE.MOUNT.UPDATE	SYSPROG SYSPROG from MVMVS
MPATH (Alias: MCHANNEL)	*prefix.sysid*.RESOLVE.MPATH.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
MSTORAGE	*prefix.sysid*.RESOLVE.MSTORAGE.LIST	SYSPROG SYSPROG from MVMVS
MTP	*prefix.sysid*.RESOLVE.MTP.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
NUCLEUS	*prefix.sysid*.RESOLVE.NUCLEUS.LIST	SYSPROG SYSPROG from MVMVS
OKSWAP	*prefix.sysid*.RESOLVE.OKSWAP.UPDATE	SYSPROG SYSPROG from MVMVS
PAGING	*prefix.sysid*.RESOLVE.PAGING.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
PARMLIST (Alias: PLIST)	*prefix.sysid*.RESOLVE.PARMLIST.LIST	SYSPROG SYSPROG from MVMVS
PCPU	*prefix.sysid*.RESOLVE.PCPU.LIST	SYSPROG SYSPROG from MVMVS
PFKEY	*prefix.sysid*.RESOLVE.PFKEY.LIST	SYSPROG
PIO	*prefix.sysid*.RESOLVE.PIO.LIST	SYSPROG SYSPROG from MVMVS
PPT*	*prefix.sysid*.RESOLVE.PPT.LIST *prefix.sysid*.RESOLVE.PPT.UPDATE	SYSPROG SYSPROG from MVMVS
PRIVATE (Alias: PVT)	*prefix.sysid*.RESOLVE.PRIVATE.LIST	SYSPROG SYSPROG from MVMVS

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
PROGRESS	*prefix.sysid*.RESOLVE.PROGRESS.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
PRSM	*prefix.sysid*.RESOLVE.PRSM.LIST	SYSPROG SYSPROG from MVMVS
REALLOC (Alias: RA)	*prefix.sysid*.RESOLVE.REALLOC.UPDATE	SYSPROG
REPLIES	*prefix.sysid*.RESOLVE.REPLIES.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
RESERVES	*prefix.sysid*.RESOLVE.RESERVES.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
RSM	*prefix.sysid*.RESOLVE.RSM.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
SDUMP	*prefix.sysid*.RESOLVE.SDUMP.UPDATE	SYSPROG SYSPROG from MVMVS
SETOP	*prefix.sysid*.RESOLVE.SETOP.LIST	SYSPROG SYSPROG from MVMVS
SMFEXIT*	*prefix.sysid*.RESOLVE.SMFEXIT.LIST *prefix.sysid*.RESOLVE.SMFEXIT.UPDATE	SYSPROG SYSPROG from MVMVS
SMSLIST	*prefix.sysid*.RESOLVE.SMSLIST.LIST	SYSPROG SYSPROG from MVMVS
SOFTFRR	*prefix.sysid*.RESOLVE.SOFTFRR.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
SPACE	*prefix.sysid*.RESOLVE.SPACE.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
SRM	*prefix.sysid*.RESOLVE.SRM.LIST	SYSPROG SYSPROG from MVMVS SYSPROG from AAO
SSVT* (Alias: SSCT)	*prefix.sysid*.RESOLVE.SSVT.LIST *prefix.sysid*.RESOLVE.SSVT.UPDATE	SYSPROG SYSPROG from MVMVS
STATUS	*prefix.sysid*.RESOLVE.STATUS.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
SUBMIT	*prefix.sysid*.RESOLVE.SUBMIT.UPDATE	SYSPROG
SVCFIND	*prefix.sysid*.RESOLVE.SVCFIND.LIST	SYSPROG SYSPROG from MVMVS
SYSDUMP	*prefix.sysid*.RESOLVE.SYSDUMP.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
TCB	*prefix.sysid*.RESOLVE.TCB.LIST	SYSPROG SYSPROG from MVMVS
TERM	*prefix.sysid*.RESOLVE.TERM.LIST	SYSPROG SYSPROG from MVMVS
TIME	*prefix.sysid*.RESOLVE.TIME.LIST	SYSPROG SYSPROG from MVMVS
TIOT	*prefix.sysid*.RESOLVE.TIOT.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
TPIO	*prefix.sysid*.RESOLVE.TPIO.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
TQE	*prefix.sysid*.RESOLVE.TQE.LIST	SYSPROG SYSPROG from MVMVS
TRACK	*prefix.sysid*.RESOLVE.TRACK.LIST	SYSPROG

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
TRTBL	*prefix.sysid*.RESOLVE.TRTBL.LIST	SYSPROG SYSPROG from MVMVS
TSULIST	*prefix.sysid*.RESOLVE.TSULIST.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
UCB	*prefix.sysid*.RESOLVE.UCB.LIST	SYSPROG SYSPROG from MVMVS
UNLOAD	*prefix.sysid*.RESOLVE.UNLOAD.UPDATE	SYSPROG SYSPROG from MVMVS
USING	*prefix.sysid*.RESOLVE.USING.LIST	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
VIO	*prefix.sysid*.RESOLVE.VIO.LIST	SYSPROG SYSPROG from MVMVS
VMCMD	*prefix.sysid*.RESOLVE.VMCMD.UPDATE	SYSPROG SYSPROG from AAO SYSPROG from MVMVS
WAITING	*prefix.sysid*.RESOLVE.WAITING.LIST	SYSPROG SYSPROG from MVMVS
WARNING (Alias: AEW and PW)	*prefix.sysid*.RESOLVE.WARNING.LIST	SYSPROG SYSPROG from MVMVS
XCALL	Secures who can issue the MAINVIEW SYSPROG Services XCALL service. **Note:** Use only if requested by BMC Software Customer Support personnel. **Resource Name:** *prefix.sysid*.RESOLVE.XCALL.UPDATE	SYSPROG

* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
XLOAD	Secures who can issue the MAINVIEW SYSPROG Services XLOAD service. **Note:** Use only if requested by BMC Software Customer Support personnel. *prefix.sysid*.RESOLVE.XLOAD.LIST	SYSPROG
XSERVICE	Secures who can issue the MAINVIEW SYSPROG Services XSERVICE service. **Note:** Use only if requested by BMC Software Customer Support personnel. *prefix.sysid*.RESOLVE.XSERVICE.LIST	SYSPROG
ZAP	*prefix.sysid*.RESOLVE.ZAP.UPDATE	SYSPROG SYSPROG from MVMVS
The following lists COMMON STORAGE MONITOR services you can access from MAINVIEW for MVS.		
OVERVIEW	*prefix.sysid*.CSMON.OVERVIEW.LIST	COMMON STORAGE MONITOR SYSPROG from MVMVS
SUMMARY	*prefix.sysid*.CSMON.SUMMARY.LIST	COMMON STORAGE MONITOR SYSPROG from MVMVS
STATUS	*prefix.sysid*.CSMON.STATUS.LIST	COMMON STORAGE MONITOR SYSPROG from MVMVS
DISPLAY	*prefix.sysid*.CSMON.DISPLAY.LIST	COMMON STORAGE MONITOR SYSPROG from MVMVS
* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.		

Table 2. Resources for MAINVIEW SYSPROG Services (Continued)

Service	Resource name	Affects products
ALTER	*prefix.sysid*.CSMON.ALTER.UPDATE	COMMON STORAGE MONITOR SYSPROG from MVMVS
FREE	*prefix.sysid*.CSMON.FREE.UPDATE	COMMON STORAGE MONITOR SYSPROG from MVMVS
* An exit can be used to modify the *function* qualifier (see page18) in the resource name for any service, as described on page 100. A default exit is provided for services marked with an asterisk in this table.		

Resources Common to MAINVIEW for CICS and the AutoOPERATOR for CICS Option

Table 3 lists the resources that, once secured, affect both MAINVIEW for CICS and the AutoOPERATOR for CICS option. Refer to "Resources for MAINVIEW for CICS" on page 54 for more resources that affect the MAINVIEW for CICS product.

Note: In this table, the AutoOPERATOR for CICS option has been abbreviated to AO for CICS. See page 17 for an explanation of the resource naming convention.

Table 3. CICS Action Services

Action	Description	Affects products
CLASSES		
ALTER MAXT	Secures access to the ALTER MAXT action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTMAXT	MAINVIEW for CICS AO for CICS
ALTER AMXT	Secures access to the ALTER AMXT action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTAMXT	MAINVIEW for CICS AO for CICS
ALTER CLASS 1	Secures access to the ALTER CLASS 1 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM001	MAINVIEW for CICS AO for CICS
ALTER CLASS 2	Secures access to the ALTER CLASS 2 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM002	MAINVIEW for CICS AO for CICS
ALTER CLASS 3	Secures access to the ALTER CLASS 3 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM003	MAINVIEW for CICS AO for CICS
ALTER CLASS 4	Secures access to the ALTER CLASS 4 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM004	MAINVIEW for CICS AO for CICS
ALTER CLASS 5	Secures access to the ALTER CLASS 5 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM005	MAINVIEW for CICS AO for CICS
ALTER CLASS 6	Secures access to the ALTER CLASS 6 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM006	MAINVIEW for CICS AO for CICS

Table 3. CICS Action Services (Continued)

Action	Description	Affects products
ALTER CLASS 7	Secures access to the ALTER CLASS 7 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM007	MAINVIEW for CICS AO for CICS
ALTER CLASS 8	Secures access to the ALTER CLASS 8 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM008	MAINVIEW for CICS AO for CICS
ALTER CLASS 9	Secures access to the ALTER CLASS 9 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM009	MAINVIEW for CICS AO for CICS
ALTER CLASS 10	Secures access to the ALTER CLASS 10 action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTCM010	MAINVIEW for CICS AO for CICS
ALTER ICV	Secures access to the ALTER ICV action on the CLASSES display. It also secures the IMFEXEC CICS ALTER command. **Resource Name:** *prefix.ssid*.CICS.target.ALTCLAS.ALTICV	MAINVIEW for CICS AO for CICS
CONNECTION		
ACQUIRE	Secures access to the ACQUIRE connection service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.ACQCONN	MAINVIEW for CICS
RELEASE	Secures access to the RELEASE connection service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.RELCONN	MAINVIEW for CICS
INSERVE	Secures access to the INSERVE connection service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.INSERVE	MAINVIEW for CICS
OUTSERVE	Secures access to the OUTSERVE connection service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.OUTSERVE	MAINVIEW for CICS
NOTCONN	Secures access to the NOTCONN connection service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.NOTCONN	MAINVIEW for CICS
PURGE	Secures access to the PURGE connection service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.PURCONN	MAINVIEW for CICS

Table 3. CICS Action Services (Continued)

Action	Description	Affects products
CONTROLLER		
INSERVE	Secures access to the INSERVE controller service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.INSCONT	MAINVIEW for CICS
OUTSERVE	Secures access to the OUTSERVE controller service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.OUTCONT	MAINVIEW for CICS
DESTINATION		
DISABLE	Secures access to the DISABLE action on the DEST display. It also secures the IMFEXEC CICS DISABLE DEST command. **Resource Name:** *prefix.ssid*.CICS.target.ALTDEST.DISDEST	MAINVIEW for CICS AO for CICS
ENABLE	Secures access to the ENABLE action on the DEST display. It also secures the IMFEXEC CICS ENABLE DEST command. **Resource Name:** *prefix.ssid*.CICS.target.ALTDEST.ENADEST	MAINVIEW for CICS AO for CICS
PURGE TD	Secures access to the PURGE TD action on the DEST display. It also secures the IMFEXEC CICS PURGE DEST command. **Resource Name:** *prefix.ssid*.CICS.target.ALTDEST.PURGETD	MAINVIEW for CICS AO for CICS
DL/1 DATABASE		
START	Secures access to the START action in the DDIR services. It also secures the IMFEXEC CICS STARTDB command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.STADLID	MAINVIEW for CICS AO for CICS
STOP	Secures access to the STOP action in the DDIR services. It also secures the IMFEXEC CICS STOPDB command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.STODLID	MAINVIEW for CICS AO for CICS
DUMP	Secures access to the DUMP DL/1 database service. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.DUMDLID	MAINVIEW for CICS
RECOVER	Secures access to the RECOVER action in the DDIR services. It also secures the IMFEXEC CICS RECOVERDB command. **Resource Name:** *prefix.ssid*.CICS.target.ALTDEST.RECDLID	MAINVIEW for CICS AO for CICS

Table 3. CICS Action Services (Continued)

Action	Description	Affects products
FILE		
DISABLE	Secures access to the DISABLE action of the FILE, DSNAMES, and DATATABL services. It also secures the IMFEXEC CICS DISABLE FILE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.DISFILE	MAINVIEW for CICS AO for CICS
ENABLE	Secures access to the ENABLE action of the FILE, DSNAMES, and DATATABL services. It also secures the IMFEXEC CICS ENABLE FILE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.ENAFILE	MAINVIEW for CICS AO for CICS
OPEN	Secures access to the OPEN action of the FILE, DSNAMES, and DATATABL services. It also secures the IMFEXEC CICS OPEN FILE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.OPEN	MAINVIEW for CICS AO for CICS
CLOSE	Secures access to the CLOSE action of the FILE, DSNAMES, and DATATABL services. It also secures the IMFEXEC CICS CLOSE FILE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.CLOSE	MAINVIEW for CICS AO for CICS
ALLOCATE	Secures access to the IMFEXEC CICS ALLOCATE FILE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.ALLOC	AO for CICS
FREE	Secures access to the FREE action of the FILE, DSNAMES, and DATATABL services. It also secures the IMFEXEC CICS FREE FILE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTFILE.FREE	MAINVIEW for CICS AO for CICS
ICE		
PURGE ICE	Secures access to the PURGE ICE action of the ICE service. It also secures the IMFEXEC CICS PURGE ICE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTICES.PURGEICE	MAINVIEW for CICS AO for CICS
AID		
PURGE AID	Secures access to the PURGE action of the AID service. It also secures the IMFEXEC CICS PURGE AID command. **Resource Name:** *prefix.ssid*.CICS.target.ALTAID.PURGEAID	MAINVIEW for CICS

Table 3. CICS Action Services (Continued)

Action	Description	Affects products
TSUT		
PURGE TS	Secures access to the PURGE action of the TSUT service. It also secures the IMFEXEC CICS PURGE TSUT command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTSUT.PURGETS	MAINVIEW for CICS
LINE		
INSERVE	Secures access to the INSERVE line service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.INSLINE	MAINVIEW for CICS
OUTSERVE	Secures access to the OUTSERVE line service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.OUTLINE	MAINVIEW for CICS
MODES		
MAX SESSIONS	Secures access to the MAX SESSIONS modes service. **Resource Name:** *prefix.ssid*.CICS.target.ALTCONN.AVAMODE	MAINVIEW for CICS
PROGRAM		
CICSKEY	Secures access to the CICS KEY program service. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.CICSPROG	MAINVIEW for CICS
DISABLE	Secures access to the DISABLE action of the PROGRAM service. It also secures the IMFEXEC CICS DISABLE PROGRAM command. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.DISPROG	MAINVIEW for CICS AO for CICS
DROP	Secures access to the DROP action of the PROGRAM service. It also secures the IMFEXEC CICS DROP command. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.PGMDROP	MAINVIEW for CICS AO for CICS
ENABLE	Secures access to the ENABLE action of the PROGRAM service. It also secures the IMFEXEC CICS ENABLE PROGRAM command. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.ENAPROG	MAINVIEW for CICS AO for CICS
LOAD	Secures access to the LOAD action of the PROGRAM service. It also secures the IMFEXEC CICS LOAD PROGRAM command. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.PGMLOAD	MAINVIEW for CICS AO for CICS
NEWCOPY	Secures access to the NEWCOPY action of the PROGRAM service. It also secures the IMFEXEC CICS NEWCOPY PROGRAM command. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.NEWCOPY	MAINVIEW for CICS AO for CICS

Table 3. CICS Action Services (Continued)

Action	Description	Affects products
USERKEY	Secures access to the USERKEY program service. **Resource Name:** *prefix.ssid*.CICS.target.ALTPROG.USEPROG	MAINVIEW for CICS
STORAGE		
ALTER	Secures access to the ALTER action of the STORAGE service. It also secures the IMFEXEC CICS ALTERVS command. **Resource Name:** *prefix.ssid*.CICS.target.ALTER.ALTERVS	MAINVIEW for CICS AO for CICS
TASK		
INDEPENDENT KILL	Secures access to the INDEPENDENT KILL action of the TASK, ENQUEUE, TERMINAL, CONSOLES, and CONNXPND services. It also secures the IMFEXEC CICS KILL command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTASK.KILL	MAINVIEW for CICS AO for CICS
KILL	Secures access to the KILL action of the TASK, ENQUEUE, TERMINAL, CONSOLES, and CONNXPND services. It also secures the IMFEXEC CICS KILL command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTASK.KILCEMT	MAINVIEW for CICS AO for CICS
TERMINAL		
ACQUIRE	Secures access to the ACQUIRE action of the TERMINAL and CONSOLES services. It also secures the IMFEXEC CICS ACQUIRE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.ACQTERM	MAINVIEW for CICS AO for CICS
RELEASE	Secures access to the RELEASE action of the TERMINAL and CONSOLES services. It also secures the IMFEXEC CICS RELEASE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.RELTERM	MAINVIEW for CICS AO for CICS
INSERVE	Secures access to the INSERVE action of the TERMINAL and CONSOLES services. It also secures the IMFEXEC CICS INSERVE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.INSTERM	MAINVIEW for CICS AO for CICS
OUTSERVE	Secures access to the OUTSERVE action of the TERMINAL and CONSOLES services. It also secures the IMFEXEC CICS OUTSERVE command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTERM.OUTTERM	MAINVIEW for CICS AO for CICS

Table 3. CICS Action Services (Continued)

Action	Description	Affects products
TRANSACTION		
CICSKEY	Secures access to the CICSKEY transaction service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTRAN.CICTRAN	MAINVIEW for CICS
DISABLE	Secures access to the DISABLE action of the TRAN service. It also secures the IMFEXEC CICS DISABLE TRAN command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTRAN.CICTRAN	MAINVIEW for CICS AO for CICS
ENABLE	Secures access to the ENABLE action of the TRAN service. It also secures the IMFEXEC CICS ENABLE TRAN command. **Resource Name:** *prefix.ssid*.CICS.target.ALTTRAN.ENATRAN	MAINVIEW for CICS AO for CICS
NONPURGE	Secures access to the NONPURGE transaction service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTRAN.NONTRAN	MAINVIEW for CICS
PURGE	Secures access to the PURGE transaction service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTRAN.PURTRAN	MAINVIEW for CICS
USERKEY	Secures access to the USERKEY transaction service. **Resource Name:** *prefix.ssid*.CICS.target.ALTTRAN.USETRAN	MAINVIEW for CICS

Resources for AutoOPERATOR: Advanced Security

To implement advanced security for AutoOPERATOR, you must secure the appropriate resources listed in Table 1 on page 20 before you can implement security for the additional resources listed in Table 4. Implementing security at this level is an optional, additional step.

AutoOPERATOR product security can be implemented with up to five additional features and you can implement security for any or all five features by following the three-phase process described earlier in the book.

Table 4. List of Features for AutoOPERATOR Advanced Security

Feature name	Description
APPL	Applies to AutoOPERATOR applications. This feature allows you to secure who can access AutoOPERATOR applications within a terminal session such as • AutoOPERATOR Basic Automation applications (the Rules Processor application, the ALERTs applications, the CSM application, and so on) • AutoOPERATOR Advanced Automation applications (the OSPI application, EXEC Testing Facility, the Shared Object Facility, and so on) • AutoOPERATOR for MVS option applications • AutoOPERATOR for IMS option applications • AutoOPERATOR for CICS option applications • AutoOPERATOR ACCESS NV option applications **Note:** Security checking is limited to eight characters each for commands, keywords, and parameters. For more information, refer to "Resources for AutoOPERATOR Applications: (FEATURE=APPL)" on page 44.
CMD	Applies to commands you can issue from an AutoOPERATOR terminal session. This feature allows you to secure • IMS transactions by transaction name • IMS commands by command name • CICS transactions by command, keyword, and parameter • MVS commands by command and parameter **Note:** Security checking is limited to eight characters each for commands, keywords, and parameters. For more information, refer to "Resources for AutoOPERATOR Commands and Transactions: (FEATURE=CMD)" on page 49.
ALRT	Allows you to secure who can delete specific ALERTs or ALERT queues by ALERT queue name. **Note:** Security checking is limited to eight characters each for commands, keywords, and parameters. For more information, refer to "Resources for AutoOPERATOR ALERTs: (FEATURE=ALRT)" on page 51.

Table 4. List of Features for AutoOPERATOR Advanced Security (Continued)

Feature name	Description
EXEC	Allows you to secure who can schedule EXECs by EXEC name from a terminal session. You can explicitly grant authority to certain users to be able to (or not be able to) schedule specific EXECs. **Note:** Security checking is limited to eight characters each for commands, keywords, and parameters. For more information, refer to "Resources for AutoOPERATOR EXECs: (FEATURE=EXEC)" on page 51.
PARM	Allows you to secure who can have read-only access or update access to members in the Dynamic Parameter Manager application. **Note:** Security checking is limited to eight characters each for commands, keywords, and parameters. For more information, refer to "Resources for AutoOPERATOR Parameter Data: (FEATURE=PARM)" on page 52.

Important

Security implemented at this level with any of the five features might **override** security you may have implemented from resources listed in Table 1 on page 20.

For example, you may deny access to a user to issue MVS commands (with the *prefix.ssid.*AAO.target.MVSCMD resource). However, if you grant access to this user for a specific MVS command, for example:

*prefix.ssid.*AAO.target.MVSCMD.DISPLAY.ALL

this access will be allowed.

Each of these advanced security features can be implemented independently of each other or in any combination. For example, you may choose to secure AutoOPERATOR EXECs by EXEC name and secure access to AutoOPERATOR applications, but not to secure any of the other features.

The following sections describe all the resources associated with each feature.

Resources for AutoOPERATOR Applications: (FEATURE=APPL)

By specifying additional AutoOPERATOR product security with the application (APPL) feature, you can secure the ability to access AutoOPERATOR applications in a BBSEC member. See "Activating Basic Security" on page 91 for more information.

Before you can implement this AutoOPERATOR APPL-level security, you must implement security for these resources:

- *prefix.ssid.*BBI.target.ACCESS
- *prefix.ssid.*AAO.target.RULEREAD
- *prefix.ssid.*AAO.target.RULEUPD
- *prefix.ssid.*AAO.target.PARMREAD
- *prefix.ssid.*AAO.target.PARMUPD
- *prefix.ssid.*AAO.target.EXEC

Additionally, you can secure the resources listed in Table 5 for greater granularity in securing access to AutoOPERATOR applications.

See Table 10 on page 87 for a list of CLISTs you can use to help identify resources for APPL-level security.

Table 5. AutoOPERATOR Resources: Application-Level Security

What you can secure	Description
Access to the Rules Processor application	
Read access	You can secure access to the AutoOPERATOR Rules Processor application by specifying that a user cannot display the application or can access it in update or read-only mode. For users who do have access to the Rules Processor application, you may want to be able to specify who can access and take actions within the Rules Processor application and who can only read and browse the application without taking any actions. To specify read-only access, use these resource names. **Resource Name:** *prefix.ssid.*AAO.target.RULEREAD
Update access	Granting update access allows you to turn automation on and off, create rules, delete rules, enable or disable rule sets (and rules), and so on. If you grant update access, you must also explicitly grant read access. To specify update access, use these resource names. **Resource Name:** *prefix.ssid.*AAO.target.RULEUPD *prefix.ssid.*AAO.target.APPL.RULES

Table 5. AutoOPERATOR Resources: Application-Level Security (Continued)

What you can secure	Description
Update the Event Statistics application	You can limit a user to displaying the Event Statistics application and viewing all the statistics the application has accumulated and prohibit the creating of rules from this panel. For example, if a user has access to the Rules Processor Event Statistics application but you do not have authority to create rules, you can only view the application and not take any action. **Resource Name:** *prefix.ssid.*AAO.target.RULEUPD *prefix.ssid.*AAO.target.APPL.EVTSTATS
Access to specific ALERT Management applications	
ALERT Status application	You can limit which users have access to the various AutoOPERATOR ALERT management applications. You can also secure access to specific ALERTs and ALERT queues either in addition to these resources or independently. Refer to "Resources for AutoOPERATOR ALERTs: (FEATURE=ALRT)" on page 51 for more information. **Resource Name:** *prefix.ssid.*AAO.target.APPL.ALS.STATS
ALERT Overview application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.ALS.OVERVIEW
ALERT Detail application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.ALS.DETAIL
Access to the EXEC Management Application	
EXEC Manager application	You can secure access to the EXEC Manager application as well as access to certain functions within the application. You can also secure the ability to schedule specific EXECs from the COMMAND line and from the AutoOPERATOR EXEC Manager application either in addition to these resources or independently. Refer to "Resources for AutoOPERATOR EXECs: (FEATURE=EXEC)" on page 51 for more information. **Resource Name:** *prefix.ssid.*AAO.target.APPL.EXECMGR
EXEC Testing Facility	**Resource Name:** *prefix.ssid.*AAO.target.APPL.EXECTEST
Viewing variables within the EXEC Testing Facility	**Resource Name:** *prefix.ssid.*AAO.target.APPL.EXECVAR
Browsing the EXEC	**Resource Name:** *prefix.ssid.*AAO.target.APPL.EXEBRWS

Table 5. AutoOPERATOR Resources: Application-Level Security (Continued)

What you can secure	Description
Access to the Continuous State Manager application	
CSM application	You may want to secure access to the AutoOPERATOR &xsm. application which allows you to handle IPLs, shutdowns, and the management of individual objects in your system automatically. **Resource Name:** *prefix.ssid.*AAO.target.APPL.CSM.ADMIN *prefix.ssid.*AAO.target.APPL.CSM.OPER *prefix.ssid.*AAO.target.APPL.CSM.PLEX
Access to the Automation Reporter application	
Automation Reporter application	You may want to secure access to the AutoOPERATOR Automation Reporter application, which allows you to monitor automation performance on your system. **Resource Name:** *prefix.ssid.*AAO.target.APPL.AR
Access to the Shared Object Facility	
Shared Object Facility	You may want to secure access to the AutoOPERATOR Shared Object Facility. **Resource Name:** *prefix.ssid.*AAO.target.APPL.SOF
Access to the Open Systems Procedural Interface	
OSPI application	You may want to secure access to the OSPI application where you can write OSPI EXECs and communicate with VTAM-based applications. **Resource Name:** *prefix.ssid.*AAO.target.APPL.OSPI
Access to the Time-Initiated EXEC Requests facility	
TI application	You may want to secure access to the Time-Initiated EXEC Requests facility, which allows you to schedule EXECs based on the time of day. **Resource Name:** *prefix.ssid.*AAO.target.APPL.TI
Access to the AutoOPERATOR for MVS option applications	
SYSTEM STATUS application	You can limit which users have access to the individual AutoOPERATOR for MVS applications. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MVS.STATUS
OPERATOR REQUESTS application	Secures access to the OPERATOR REQUESTS application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MVS.OPER
ADDRESS SPACES application	Secures access to the ADDRESS SPACES application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MVS.ADSPACE
ENQUEUE/RESERVE application	Secures access to the ENQUEUE/RESERVE application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MVS.ENQ

Table 5. AutoOPERATOR Resources: Application-Level Security (Continued)

What you can secure	Description
TAPE STATUS/CONTROL application	Secures access to the TAPE STATUS/CONTROL application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MVS.DEVICES
DASD STATUS/CONTROL application	Secures access to the DASD STATUS/CONTROL application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MVS.DEVICES
VTAM MAJOR NODES application	Secures access to the VTAM MAJOR NODES application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.MAJNODE
VTAM APPLICATIONS application	Secures access to the VTAM APPLICATIONS application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.APPLS
VTAM CDRMS application	Secures access to the VTAM CDRMS application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.CDRMS
VTAM CDRSCS application	Secures access to the VTAM CDRSCS application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.CDRSCS
VTAM LINES application	Secures access to the VTAM LINES application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.LINES
VTAM CLUSTERS application	Secures access to the VTAM CLUSTERS application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.CLSTRS
VTAM TERMINALS application	Secures access to the VTAM TERMINALS application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.VTAM.TERMS
Access to AutoOPERATOR for CICS option applications	
CICS Status application	You can limit which users have access to the individual AutoOPERATOR for CICS option applications. **Resource Name:** *prefix.ssid.*AAO.target.APPL.CICS.STATUS
CICS Broadcast application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.CICS.BRDCST
Access to the AutoOPERATOR for IMS option applications	
IMS REGIONS application	You can limit which users have access to the AutoOPERATOR for IMS applications. **Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.REGIONS
IMS DATABASE application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.DATABASE
IMS STATUS application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.STATUS

Table 5. AutoOPERATOR Resources: Application-Level Security (Continued)

What you can secure	Description
IMS AREA application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.AREA
IMS DEDB application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.DEDB
IMS ISC application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.ISC
IMS LINES application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.LINES
IMS LTERMS application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.LTERMS
IMS MSDB application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.MSDB
IMS NODES application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.NODES
IMS PROGRAM application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.PROGRAM
IMS REGION application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.REGION
IMS RTCODE application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.RTCODE
IMS TRANSACTION application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.TRAN
IMS NETWORK application	**Resource Name:** *prefix.ssid.*AAO.target.APPL.IMS.NET
Access to the AutoOPERATOR ACCESS NV option applications	
ACCESS NV	You can limit which users have access to the NetView Operator Workstation application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.ANV
Access to the TapeSHARE for AutoOPERATOR option	
TapeSHARE Workstation	You can limit which users have access to the TapeSHARE Workstation application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.TAPSHR
Access to the AutoOPERATOR for MQSeries option	
AutoOPERATOR for MQSeries Workstation	You can limit which users have access to the AutoOPERATOR for MQSeries Workstation application. **Resource Name:** *prefix.ssid.*AAO.target.APPL.MQSERIES

Resources for AutoOPERATOR Commands and Transactions: (FEATURE=CMD)

By specifying additional AutoOPERATOR product security with the command (CMD) feature, you can secure the ability to issue specific commands and transactions from AutoOPERATOR terminal sessions.

Before you can implement this AutoOPERATOR CMD-level security, you must implement security for these resources:

- *prefix.ssid.*BBI.target.ACCESS
- *prefix.ssid.*BBI.target.BBICMD
- *prefix.ssid.*AAO.target.MVSCMD
- *prefix.ssid.*AAO.target.CICSTRAN
- *prefix.ssid.*AAO.target.IMSTRAN
- *prefix.ssid.*AAO.target.IMSCMD
- *prefix.ssid.*AAO.target.IMSMSG
- *prefix.ssid.*AAO.target.RESAUTH

Additionally, you can secure the resources listed in Table 6 for greater granularity in securing commands and transactions.

See Table 10 on page 87 for a list of CLISTs you can use to help identify resources for CMD-level security.

Table 6. AutoOPERATOR Resources: Command-Level Security

What you can secure	Description
Invoking CICS transactions	Secures invoking of specific CICS transactions from an AutoOPERATOR terminal session by CICS transaction name. You must create a separate security definition for each CICS transaction that you secure. **Resource Name:** *prefix.ssid.*AAO.target.CICSTRAN.command This resource name may include a command name that is more than eight characters long, but security checking checks **only the first eight characters of the command name.**
Invoking IMS transactions	Secures invoking of specific IMS transactions from an AutoOPERATOR terminal session by IMS transaction name. You must create a separate security definition for each IMS transaction that you secure. **Resource Name:** *prefix.ssid.*AAO.target.IMSTRAN.command This resource name may include a transaction name that is more than eight characters long, but security checking checks **only the first eight characters of the command and the first eight bytes of each parameter (if any).**

Table 6. AutoOPERATOR Resources: Command-Level Security (Continued)

Invoking IMS commands	Secures invoking of specific IMS commands from an AutoOPERATOR terminal session by IMS command name and two parameters. You must create a separate security definition for each IMS command and parameter that you secure. **Note:** If you are securing these resources in a security class of DATASET, the ESM will not check the value of the two parameters. Only the command name is checked. **Resource Name:** *prefix.ssid*.AAO.target.IMSCMD.command.parameter.parameter This resource name may include command names and parameter names that are more than eight characters long, but security checking checks **only the first eight characters of the command and the first eight bytes of each parameter (if any)**.
Invoking MVS commands	Secures invoking of specific MVS commands from an AutoOPERATOR terminal session by MVS command name and one parameter. **Note:** If you are securing these resources in a security class of DATASET, the ESM will not check the value of the command and the parameter. Only the command name is checked. You must create a separate security definition for each MVS command and parameter that you secure. **Resource Name:** *prefix.ssid*.AAO.target.MVSCMD.command.parameter This resource name may include command names and parameter names that are more than eight characters long, but security checking checks **only the first eight characters of the command name and additional parameter names.**

Resources for AutoOPERATOR ALERTs: (FEATURE=ALRT)

By choosing the ALRT feature of AutoOPERATOR-level security, you are choosing to secure a user's ability to delete ALERTs and ALERT queues through the AutoOPERATOR ALERT Detail and AutoOPERATOR ALERT STATS applications.

The resource names are as follows:

- *prefix.ssid.*AAO.target.ALRT.DE.*queuename*

  Use this resource to secure ALERTs by their queue name. Every AutoOPERATOR ALERT belongs to a queue so, if you grant access to this resource, ALERTs within the queue can be deleted from the ALERT Detail application. If you deny access to an ALERT queue with this resource, the ALERTs within that queue cannot be deleted.

- *prefix.ssid.*AAO.target.ALRT.DEQ.*queuename*

  Use this resource to secure ALERT queues. If you grant access to this resource, the entire ALERT queue can be deleted from the ALERT STATS application. Any ALERTs within the queue are also deleted. If you deny access, the user cannot delete the queue.

See Table 10 on page 87 for a list of CLISTs you can use to help identify resources for ALRT-level security.

Resources for AutoOPERATOR EXECs: (FEATURE=EXEC)

You can specify that you want to secure the ability to create and schedule, edit, and test AutoOPERATOR EXECs by AutoOPERATOR EXEC name. Before you can implement this AutoOPERATOR EXEC-level security, you must implement security for these resources (see Table 1 on page 20).

The resource name is *prefix.ssid.*AAO.target.EXEC.

By choosing the EXEC feature of AutoOPERATOR-level security, you are choosing to secure a user's ability to schedule EXECs by EXEC name from the COMMAND line during a user’s terminal session.

The resource name is *prefix.ssid.*AAO.target.EXEC.execname.

With this resource, you are also securing a user’s ability to access the EXEC from within the EXEC Manager application. This limits

- Selecting a specific EXEC for testing
- Scheduling a specific EXEC
- Browsing a specific EXEC
- Disabling a specific EXEC

When securing EXECs, it is important to note that, with only a few exceptions, **the actions scheduled within the EXEC are not secured.** For example, you may secure the ability to issue MVS commands from a specific user. However, if you allow the user to have access to an EXEC that issues an MVS command, the EXEC and the MVS command will be allowed to run completely.

There are two exceptions:

- If you secure the ability to access CICS services through the BBI-SS PAS (as seen in "Resources Common to MAINVIEW for CICS and the AutoOPERATOR for CICS Option" on page 35), some CICS action services have IMFEXEC CICS statements for the AutoOPERATOR for CICS option.

  These IMFEXEC CICS statements can be secured and, if they are, these restrictions **are valid in an EXEC that uses these statements.**

- If you secure MAINVIEW SYSPROG Services services

  You can invoke MAINVIEW SYSPROG Services services in an EXEC with an IMFEXEC RES statement. If the MAINVIEW SYSPROG Services service is secured, the restrictions **are valid in an EXEC that uses these statements.**

See Table 10 on page 87 for a list of CLISTs you can use to help identify resources for EXEC-level security.

Resources for AutoOPERATOR Parameter Data: (FEATURE=PARM)

By choosing the PARM feature of AutoOPERATOR-level security, you are choosing to secure a user's ability to update, read, delete, add, or activate AutoOPERATOR parameter members through the AutoOPERATOR Dynamic Parameter Manager application.

The resource names are as follows:

- *prefix.ssid.*AAO.target.PARMREAD.membername

  Allows you to specify individual members allowing read-only access.

- *prefix.ssid.*AAO.target.PARMUPD.membername

  Allows you to specify individual members allowing update access. Note that the maximum length of the member name is eight characters.

See Table 10 on page 87 for a list of CLISTs you can use to help identify resources for PARM-level security.

Access through an EXCP Terminal

BMC Software products allow the use of terminals that are attached directly to the host system by a channel. EXCP macros are used to communicate with such a terminal. An EXCP-driven terminal is always associated with a user ID.

To allow only specific user IDs to use predefined device addresses, a special resource is introduced in the format:

prefix.*ssid*.`BBI.TERM`.*xxxx*

where

prefix	Is a four-character maximum, user-defined prefix
ssid.	Is the BBI-SS PAS identifier (SSID)
BBI	Is a predefined literal
TERM*xxxx*	Is the literal `TERM` followed by a four-digit device address

For example, the following resource name describes a resource for the subsystem SYSB for the attached terminal device 74C:

```
BAB.SYSB.BBI.TERM.074C
```

Resources for CMF MONITOR

For information on controlling access to the views in the CMF MONITOR online component, refer to Part 3, "Enhanced Security".

For information on controlling access to the screens provided by the CMFMON component, refer to the *CMF MONITOR Customization Guide*.

Resources for MAINVIEW for CICS

Table 7 and Table 8 describe the resources that can be secured with MAINVIEW for CICS. Refer to "Resources Common to MAINVIEW for CICS and the AutoOPERATOR for CICS Option" on page 35 for a list of resources you can secure for MAINVIEW for CICS and the AutoOPERATOR for CICS option.

Table 7. CICS Display Services

Service	Description
ABEND	
ABEND	Secures access to the ABEND service display. **Resource Name:** *prefix.ssid*.CICS.target.ABEND.ABEND
AID	
AID	Secures access to the Automatic Initiate Descriptor (AID) service display. **Resource Name:** *prefix.ssid*.CICS.target.AID.AID
CLASSES	
CLASSES	Secures access to the CLASS service display. **Resource Name:** *prefix.ssid*.CICS.target.CLASS.CLASSES
TSUT	
TSUT	Secures access to the TSUT service display. **Resource Name:** *prefix.ssid*.CICS.target.TSUT.TSUT
CONNECT	
CONNECT	Secures access to the CONNECT service display. **Resource Name:** *prefix.ssid*.CICS.target.CONNECT.CONNECT
CONNXPND	Secures access to the CONNXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.CONNECT.CONNXPND
CONNXPN2	Secures access to the CONNXPN2 service display. **Resource Name:** *prefix.ssid*.CICS.target.CONNECT.CONNXPN2
SESSIONS	Secures access to the SESSIONS service display. **Resource Name:** *prefix.ssid*.CICS.target.CONNECT.SESSIONS

Table 7. CICS Display Services (Continued)

Service	Description
DB2SYSP	
DB2SYSP	Secures access to the DB2SYSP service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2SYSP.DB2SYSP
DBCTL	Secures access to the DBCTL service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2SYSP.DBCTL
MQSERIES	Secures access to the MQSERIES service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2SYSP.MQSERIES
DB2TASK	
DB2TASK	Secures access to the DB2TASK service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2TASK.DB2TASK
DB2TXPND	Secures access to the DB2TXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2TASK.DB2TXPND
DBCTASK	Secures access to the DBCTASK service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2TASK.DBCTASK
MQTASK	Secures access to the MQTASK service display. **Resource Name:** *prefix.ssid*.CICS.target.DB2TASK.MQTASK
DEST	
DEST	Secures access to the DEST service display. **Resource Name:** *prefix.ssid*.CICS.target.DEST.DEST
DL/1	
DL/1	Secures access to the DL/1 service display. **Resource Name:** *prefix.ssid*.CICS.target.DLI.DLI
DUMP	
DUMP	Secures access to the DUMP service display. **Resource Name:** *prefix.ssid*.CICS.target.DUMP.DUMP

Table 7. CICS Display Services (Continued)

Service	Description
ENQUEUE	
ENQUEUE	Secures access to the ENQUEUE service display. **Resource Name:** *prefix.ssid*.CICS.target.ENQUEUE.ENQUEUE
EXITS	
EXITS	Secures access to the EXITS service display. **Resource Name:** *prefix.ssid*.CICS.target.EXITS.EXITS
FILE	
DATATABL	Secures access to the DATATABL service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.DATATABL
DDIR	Secures access to the DDIR service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.DDIR
DDIRXPND	Secures access to the DDIRXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.DDIRXPND
DDIRXPN2	Secures access to the DDIRXPN2 service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.DDIRXPN2
DSNAMES	Secures access to the DSNAMES service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.DSNAMES
FILE	Secures access to the FILE service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.FILE
FILEXPND	Secures access to the FILEXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.FILEXPND
FILEXPN2	Secures access to the FILEXPN2 service display. **Resource Name:** *prefix.ssid*.CICS.target.FILE.FILEXPN2
TERMINAL	
CONSOLES	Secures access to the CONSOLES service display. **Resource Name:** *prefix.ssid*.CICS.target.TERM.CONSOLES
TERMINAL	Secures access to the TERMINAL service display. **Resource Name:** *prefix.ssid*.CICS.target.TERM.TERMINAL

Table 7. CICS Display Services (Continued)

Service	Description
TERMXPND	Secures access to the TERMXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.TERM.TERMXPND
HISTORY	
HISTORY	Secures access to the HISTORY service display. **Resource Name:** *prefix.ssid*.CICS.target.HISTORY.HISTORY
ICE	
ICE	Secures access to the ICE service display. **Resource Name:** *prefix.ssid*.CICS.target.ICE.ICE
JOURNAL	
JOURNAL	Secures access to the JOURNAL service display. **Resource Name:** *prefix.ssid*.CICS.target.JOURNAL.JOURNAL
MONITOR	
MONITOR	Secures access to the MONITOR service display. **Resource Name:** *prefix.ssid*.CICS.target.MONITOR.MONITOR
NUCLEUS	
LPAS	Secures access to the LPAS service display. **Resource Name:** *prefix.ssid*.CICS.target.NUCLEUS.LPAS
NUCLEUS	Secures access to the NUCLEUS service display. **Resource Name:** *prefix.ssid*.CICS.target.NUCLEUS.NUCLEUS
TCBS	Secures access to the TCBS service display. **Resource Name:** *prefix.ssid*.CICS.target.NUCLEUS.TCBS
PLAN	
PLAN	Secures access to the PLAN service display. **Resource Name:** *prefix.ssid*.CICS.target.PLAN.PLAN
PLANXPND	Secures access to the PLANXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.PLAN.PLANXPND

Table 7. CICS Display Services (Continued)

Service	Description
PPST	
PPST	Secures access to the PPST service display. **Resource Name:** *prefix.ssid*.CICS.target.PPST.PPST
PROBLEM	
PROBLEM	Secures access to the PROBLEM service display. **Resource Name:** *prefix.ssid*.CICS.target.PROBLEM.PROBLEM
CSTATUS	Secures access to the CSTATUS service display. **Resource Name:** *prefix.ssid*.CICS.target.PROBLEM.CSTATUS
STATUS	Secures access to the STATUS service display. **Resource Name:** *prefix.ssid*.CICS.target.PROBLEM.STATUS
PROGRAM	
PROGRAM	Secures access to the PROGRAM service display. **Resource Name:** *prefix.ssid*.CICS.target.PROGRAM.PROGRAM
REMOTES	Secures access to the REMOTES service display. **Resource Name:** *prefix.ssid*.CICS.target.PROGRAM.REMOTES
PSBNAME	
PSB	Secures access to the PSB service display. **Resource Name:** *prefix.ssid*.CICS.target.PSB.PSBNAME
REVIEW	
REVIEW	Secures access to the REVIEW service display. **Resource Name:** *prefix.ssid*.CICS.target.REVIEW.REVIEW
SHARE	
SHARE	Secures access to the SHARE service display. **Resource Name:** *prefix.ssid*.CICS.target.SHARE.SHARE

Table 7. CICS Display Services (Continued)

Service	Description
SUBPOOL	
DSAS	Secures access to the DSAS service display. **Resource Name:** *prefix.ssid*.CICS.target.SUBPOOL.DSAS
SCAS	Secures access to the SCAS service display. **Resource Name:** *prefix.ssid*.CICS.target.SUBPOOL.SCAS
SUBPOOL	Secures access to the SUBPOOL service display. **Resource Name:** *prefix.ssid*.CICS.target.SUBPOOL.SUBPOOL
REGIONS	Secures access to the REGIONS service display. **Resource Name:** *prefix.ssid*.CICS.target.SUBPOOL.REGIONS
SUFFIX	
SUFF	Secures access to the SUFF service display. **Resource Name:** *prefix.ssid*.CICS.target.SUFFIX.SUFF
SUMMARY	
SUMMARY	Secures access to the SUMMARY service display. **Resource Name:** *prefix.ssid*.CICS.target.SUMMARY.SUMMARY
TASK	
MEMORY	Secures access to the MEMORY service display. **Resource Name:** *prefix.ssid*.CICS.target.TASK.MEMORY
TASK	Secures access to the TASK service display. **Resource Name:** *prefix.ssid*.CICS.target.TASK.TASK
TASKXPN2	Secures access to the TASKXPN2 service display. **Resource Name:** *prefix.ssid*.CICS.target.TASK.TASKXPN2
TASKXPN3	Secures access to the TASKXPN3 service display. **Resource Name:** *prefix.ssid*.CICS.target.TASK.TASKXPN3
TASKXPN4	Secures access to the TASKXPN4 service display. **Resource Name:** *prefix.ssid*.CICS.target.TASK.TASKXPN4

Table 7. CICS Display Services (Continued)

Service	Description
TASKXPND	Secures access to the TASKXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.TASK.TASKXPND
TEMP	
TEMPSTRG	Secures access to the TEMPSTRG service display. **Resource Name:** *prefix.ssid*.CICS.target.TEMP.TEMPSTRG
TEMPXPND	Secures access to the TEMPXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.TEMP.TEMPXPND
TIOT	
TIOT	Secures access to the TIOT service display. **Resource Name:** *prefix.ssid*.CICS.target.TIOT.TIOT
VOLUMES	Secures access to the VOLUMES service display. **Resource Name:** *prefix.ssid*.CICS.target.TIOT.VOLUMES
TRAN	
TCLASS	Secures access to the TCLASS service display. **Resource Name:** *prefix.ssid*.CICS.target.TRAN.TCLASS
TCLAXPND	Secures access to the TCLAXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.TRAN.TCLAXPND
TRAN	Secures access to the TRAN service display. **Resource Name:** *prefix.ssid*.CICS.target.TRAN.TRAN
TRANXPND	Secures access to the TRANXPND service display. **Resource Name:** *prefix.ssid*.CICS.target.TRAN.TRANXPND
VTAM	
VTAM	Secures access to the VTAM service display. **Resource Name:** *prefix.ssid*.CICS.target.VTAM.VTAM

Table 8. MAINVIEW for CICS Diagnostic Services

Service	Description
DIAG	
CONFIG	Secures access to the CONFIG diagnosis service. **Resource Name:** *prefix.ssid*.CICS.target.DIAG.CONFIG
GRAFSTAT	Secures access to the GRAFSTAT diagnosis service. **Resource Name:** *prefix.ssid*.CICS.target.DIAG.GRAFSTAT
PROGSS	Secures access to the PROGSS diagnosis service. **Resource Name:** *prefix.ssid*.CICS.target.DIAG.PROGSS
QSTAT	Secures access to the QSTAT diagnosis service. **Resource Name:** *prefix.ssid*.CICS.target.DIAG.QSTAT
VALIDATE	Secures access to the VALIDATE diagnosis service. **Resource Name:** *prefix.ssid*.CICS.target.DIAG.VALIDATE

Resources for MAINVIEW for DB2

Table 9 describes the additional product security in MAINVIEW for DB2 (version 5.1 and later) with the command (CMD) feature. You can secure the ability to issue specific DB2 commands from a MAINVIEW for DB2 terminal session. Refer to Table 1 on page 20 for a list of resources shared across products.

Before you can implement CMD-level security, you must implement security for the following resource:

prefix.ssid.`BBI.target.ACCESS`

See the following table for defining resources for specific commands:

Table 9. MAINVIEW for DB2 Resources: Command-Level Security

What you can secure	Description

Invoking DB2 commands	Secures invoking of specific DB2 commands and operands from a terminal session by DB2 command name and one operand.
	
	Note: If you are securing these resources in a security class of DATASET, the ESM will not check the value of the command and the operand. Only the command name is checked.
	
	You must create a separate security definition for each DB2 command and operand that you secure.
	
	Resource Name: *prefix.ssid*.DMR.target.DB2CMD.command.operand
	
	Note: All combinations of command and operand abbreviations must be defined to secure a command; for example:
	
	`DISPLAY.THREAD`
	`DISPLAY.THD`
	`DIS.THREAD`
	`DIS.THD`

Resources for MAINVIEW for DBCTL, MAINVIEW FOCAL POINT, and MAINVIEW for IMS

At this time, there are no additional resources to be secured for MAINVIEW for DBCTL, MAINVIEW FOCAL POINT, or MAINVIEW for IMS. Refer to Table 1 on page 20 for a list of resources that are shared across products.

Resources for InTune

For InTune version 2.1 and later, refer to the *InTune User's Guide* for informaton about controlling access to InTune resources.

For InTune version 1.3 and ealier, use the information provided here to control access to InTune resources. You can secure a user's ability to access an InTune address space, monitor a specific job or subsystem, or open a data set for CSECT resolution.

To verify whether a user has access to the InTune address space, InTune uses the resource name:

prefix.ssid`.INTUNE.ACCESS`

To verify whether a user can monitor a particular job, InTune uses the resource name:

prefix.jobname`.INTUNE.MONITOR`

The resource class for all InTune resources is DATASET.

If InTune is not authorized to read certain system (LINKLIB) or user data sets, it does not attempt to read those data sets. This situation affects the CSECT resolution function of InTune. None of the modules in the restricted data sets is resolved in CSECTs. If CSECT resolution is required, the InTune started task should be granted the necessary authority to access required data sets.

Chapter 5. Configuring Your ESM for Basic Security

Once you have decided which resources to secure and created names for all the resources based on the systems and targets for which you will implement security, you can begin the task of identifying the resources to the ESM at your site.

The steps required to identify resources include

1. Defining a security class ($BOOLE) to your ESM to which all resources will belong.
2. Identifying the fully named resources to the security class.
3. Granting or denying access to the resources.

When these steps are completed, go to Chapter 7, "Activating Basic Security" on page 91 for instructions about completing implementation of security and turning it on.

Note: Refer to the IBM publication *RACF Command Language Reference* for further details on the security classes and using the RACF RDEFINE and PERMIT commands.

Defining Security Class $BOOLE

Follow these instructions to define a security class to your ESM for MAINVIEW resources. The default security class is $BOOLE.

In your RACF Router Table:

1. Enter the following TSO command:

   ```
   ICHRFRTB CLASS=$BOOLE,
            ACTION=RACF
   ICHRFRTB TYPE=END
   ```

   where `$BOOLE` is the default security class name.

In your RACF Resource Class Descriptor Table:

2. Enter:

   ```
   ICHERCDE CLASS=$BOOLE,
            ID=   ,
            FIRST=ALPHA,
            MAXLNTH=246,
            OTHER=ANY,
            OPER=NO,
            POSIT=
   ```

3. Enter the following command:

   ```
   SETROPTS CLASSACT($BOOLE)
   ```

   to activate the `$BOOLE` resource class.

4. Enter the following command:

   ```
   SETROPTS GENERIC($BOOLE)
   ```

   to allow `$BOOLE` to use generic profiles.

Once these steps are complete, creating the security class is complete. The next step is to identify all the resources to be secured to this class. This step is described in the next sections. Go to "Defining MAINVIEW Product Resources to Protect" and "Identifying MAINVIEW SYSPROG Services" on page 68 for instructions to identify resources and MAINVIEW SYSPROG Services.

Defining MAINVIEW Product Resources to Protect

How a resource is identified to an ESM (such as RACF) for protection determines whether the resource is initially available to all users. You have the option of deciding which resources will be available to which users by defining resources for protection.

For the RACF ESM, this is done with the universal access (UACC) keyword of the RDEFINE command. The UACC of any resource may be set as either

- UACC(NONE)

  This UACC restricts access to the resource, and users cannot access the resource unless the access is explicitly granted.

- UACC(READ)

  This UACC permits all users access to the resource. If you want to place restrictions on the resource, you must explicitly deny access to specific users.

Therefore, it is important for you to examine the various resources you want to secure and determine if you want a resource to be initially available to all users.

Authorizing Access

The complete syntax for securing MAINVIEW product resources for the ESM of RACF is as follows:

`REDEFINE security_class` (*prefix.ssid*`.proname.target.function) UACC(NONE)`

where

RDEFINE
: Is a RACF command entered from a TSO terminal session, ISPF panel, or batch job

security_class
: Is the RACF security class for site-defined resources

  The default security class name for MAINVIEW product resources is $BOOLE.

prefix.ssid.productname.target.function
: Is the fully named resource to secure

UACC(NONE) Secures the resource against all access until you grant users (or groups of users) access to this resource

You may choose to define resources with a universal access (UACC) of READ. The syntax for this is `UACC(READ)`. By using this parameter, the resource is not secured and all users may access this resource until you deny access.

Helpful Hint

If initially you want less restrictions, you can start out with all access granted [UACC(READ)]. Then, as you proceed, you can determine which areas need to be protected or restricted. You can do this either by redefining the resource with a UACC(NONE) and then permitting users access or by denying access on a user by user basis.

If initially you want more restrictions, you can start out with all access denied [UACC(NONE)]. Then, as you proceed, you can determine which users (or groups of users) you will grant access to.

You can also decide to have a mixed level of restrictions, by defining some resources with UACC(NONE) and others with UACC(READ).

Example: Securing MVS Commands for All Users

Suppose you want to secure MVS commands from an AutoOPERATOR terminal session. In your system, initially you want to limit access to a few people on your production system, which has an SSID of PRD1 and a default security class of $BOOLE. See Chapter 4, "Reviewing Product Resources" on page 17, for more information.

Defining this resource protection to RACF looks like this:

```
RDEFINE $BOOLE BBM.PRD1.BBI.PRD1.MVSCMD UACC(NONE)
```

This definition secures MVS commands on PRD1 from all users. MVS commands cannot be used by any user on PRD1.

To allow some users to issue MVS command authority, follow the instructions in "Granting or Denying Access" on page 69.

Example: Allowing All Users to Send Messages to the BBI-SS PAS Journal

In this example, initially you want to allow all users to have write-access to the BBI-SS PAS Journal. The production system has an SSID of PRD1. The target is PRD1, and you use the default security class of $BOOLE.

Identifying this resource to RACF looks like this:

```
RDEFINE $BOOLE BBM.PRD1.BBI.PRD1.JRNLMSG UACC(READ)
```

This definition allows all users to write messages to the BBI-SS PAS Journal.

To restrict access, follow the instructions in "Granting or Denying Access" on page 69.

Example: Allowing Mixed Accessibility

Some resource names are designed for situations where you may want all users to have read-only access and others to also have update access. For example, in the AutoOPERATOR product, there are two resource names associated with accessing the Rules Processor:

prefix.ssid`.AAO.target.RULEREAD (read-only access)`
prefix.ssid`.AAO.target.RULEUPD (update access)`

Suppose you have 15 users that need read-only access to the Rules Processor. Identifying this resource to RACF looks like this:

```
RDEFINE $BOOLE BBM.PRD1.AAO.PRD1.RULEREAD UACC(READ)
```

This definition allows all 15 users to have read access to the Rules Processor.

You can also select 3 of these 15 users to have update access. First, you must identify the update resource name to RACF:

```
RDEFINE $BOOLE BBM.PRD1.AAO.PRD1.RULEUPD UACC(NONE)
```

This resource is initially defined with a UACC(NONE), but to allow a subset of users to have access to this resource, you must grant them access explicitly. To do this, follow the instructions in "Granting or Denying Access" on page 69.

Identifying MAINVIEW SYSPROG Services

The syntax for securing MAINVIEW SYSPROG Services for RACF is

`REDEFINE security_class` (*prefix.system*`.productname.request.function)`
`UACC(NONE)`

where

RDEFINE — Is a RACF command entered from a TSO terminal session, ISPF panel, or batch job

security_class — Is the RACF security class to which the resources are defined

The default security class name is $BOOLE.

(*prefix.system*.productname.request.function)
Is the fully named MAINVIEW SYSPROG Services you want to secure

UACC(NONE) — Secures against all access until you grant users (or groups of users) access to this resource

You may choose to define resources with a universal access (UACC) of READ. The syntax for this is `UACC(READ)`. The resource is not secured and all users may access this resource until you deny access.

Securing MAINVIEW SYSPROG Services: This example initially grants access to all MAINVIEW SYSPROG Services:

```
RDEFINE $BOOLE (BBM.SYSA.RESOLVE*) UACC(READ)
```

The following example restricts access to all MAINVIEW SYSPROG Services UPDATE services.

```
RDEFINE $BOOLE (BBM.SYSA.RESOLVE.*.UPDATE) UACC(NONE)
```

Granting or Denying Access

Once the resources are identified to a security class, you can begin granting or denying access to the resources by user ID. You can also create a group user ID that represents a group at your site.

Granting Access

To grant access to a resource, use the RACF PERMIT statement as follows:

`PERMIT resource_name CLASS(security class) ACCESS(READ) ID(`*userid*`)`

where

PERMIT — Is a RACF command issued from a TSO terminal session, ISPF panel, or batch job

resource_name — Is the name of the resource

CLASS(security class) — Is the security class name

ACCESS(READ) — Is a RACF parameter specifying READ access; a value of READ means you are granting access to the resource

ID(*userid*) — Is the user ID of the person (or a group user ID) who is allowed access

Example: To grant update access for MAINVIEW SYSPROG Services to user BCVJXF1, specify the following statement:

```
PERMIT BBM.SYSA.RESOLVE.*.UPDATE CLASS($BOOLE) ACCESS(READ)
ID(BCVJXF1)
```

To authorize user ID BCVJXF1 to use both the list and update services of the MAINVIEW SYSPROG Services APF service, specify the following statement:

```
PERMIT BBM.SYSA.RESOLVE.APF.* ACCESS(READ) ID(BCVJXF1)
```

Denying Access

To deny access to a resource, use the RACF `PERMIT` statement as follows:

`PERMIT resource_name CLASS(security class) ACCESS(NONE) ID(`*userid*`)`

where

PERMIT	Is a RACF command entered from a TSO terminal session, ISPF panel, or batch job
resource_name	Is the name of the resource
CLASS(security class)	Is the security class name
ACCESS(NONE)	Is a RACF parameter specifying NONE; a value of NONE means you are denying access to a resource
ID(*userid*)	Is the user ID of the person (or a group user ID) who is denied access

Example: To deny access to user ID BCVJXF1, specify the following statement:

```
PERMIT BBM.SYSA.RESOLVE.*.UDATE CLASS($BOOLE) ACCESS(NONE) ID(BCVJXF1)
```

Creating Global Security Definitions: Using Generics

You may want to use generics to define a group of resources to your ESM or to grant/deny access to them. You must ensure that the security class you define or create in the ESM supports the use of generics before you can use them in naming resources.

An asterisk (*) can be used to represent a string of characters. A pound sign (#) can be used to represent a single character. All qualifiers in a resource name can be generic except the `prefix` node.

The appropriate use of generics depends on the security class you use. For documentation about RACF security classes, refer to the IBM publication *RACF Command Language Reference*.

Security authorization is granted to every resource that matches the qualified generic name. For example:

```
BBM.SS01.CICS.CICS01.FILE.*
```

grants access to all display file services without having to specify each one.

Listing MAINVIEW Product Resource Names

To see how protecting resources might affect other products, use the matrix on the following pages. For a description of these resources, see Chapter 4, “Reviewing Product Resources” on page 17.

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*ssid*.BBI.*target*.ACCESS	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.BBICMD	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.JRNLMSG	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.PMACC#	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.PMACCA	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.PMACCB	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.PMACCC	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.PMACCD	X	X	X	X	X	X			
prefix.*ssid*.BBI.*target*.TRACE.ALL			X						
prefix.*ssid*.BBI.*target*.TRACE.D		X	X	X	X				
prefix.*ssid*.BBI.*target*.TRACE.S		X	X	X	X				
prefix.*ssid*.BBI.*target*.TRALLOC		X	X	X	X				
prefix.*ssid*.AAO.*target*.CICSTRAN	X								
prefix.*ssid*.AAO.*target*.EXEC	X								
prefix.*ssid*.AAO.*target*.IMSCMD	X								
prefix.*ssid*.AAO.*target*.IMSMSG	X								
prefix.*ssid*.AAO.*target*.IMSTRAN	X								
prefix.*ssid*.AAO.*target*.MVSCMD	X								
prefix.*ssid*.AAO.*target*.PARMREAD	X								
prefix.*ssid*.AAO.*target*.PARMUPD	X								
prefix.*ssid*.AAO.*target*.RESAUTH	X								

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*ssid*.AAO.*target*.RULEREAD	X								
prefix.*ssid*.AAO.*target*.RULEUPD	X								
prefix.*ssid*.DMR.*target*.DB2CMD			X						
prefix.*ssid*.DMR.*target*.DB2TRACE.GENERIC			X						
prefix.*ssid*.DMR.*target*.DB2SQLAU			X						
prefix.*ssid*.DMR.*target*.DB2SQLAL			X						
prefix.*ssid*.AAO.*target*.ALRT.DE.queuename	X								
prefix.*ssid*.AAO.*target*.ALRT.DEQ.queuename	X								
prefix.*ssid*.AAO.*target*.CICSTRAN.cmd	X								
prefix.*ssid*.AAO.*target*.EXEC.execname	X								
prefix.*ssid*.AAO.*target*.IMSTRAN.command	X								
prefix.*ssid*.AAO.*target*.IMSCMD.cmd.parm.parm	X								
prefix.*ssid*.AAO.*target*.MVSCMD.cmd.parameter	X								
prefix.*ssid*.AAO.*target*.PARMREAD.membername	X								
prefix.*ssid*.AAO.*target*.PARMUPD.membername	X								
prefix.*ssid*.AAO.*target*.APPL.ALS.STATS	X								
prefix.*ssid*.AAO.*target*.APPL.ALS.OVERVIEW	X								
prefix.*ssid*.AAO.*target*.APPL.ALS.DETAIL	X								
prefix.*ssid*.AAO.*target*.APPL.ANV	X								
prefix.*ssid*.AAO.*target*.APPL.CICS.STATUS	X								
prefix.*ssid*.AAO.*target*.APPL.CICS.BRDCST	X								
prefix.*ssid*.AAO.*target*.APPL.CSM.ADMIN	X								
prefix.*ssid*.AAO.*target*.APPL.CSM.OPER	X								
prefix.*ssid*.AAO.*target*.APPL.EVTSTATS	X								
prefix.*ssid*.AAO.*target*.APPL.EXECMGR	X								

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.ssid.AAO.*target*.APPL.EXECTEST	X								
prefix.ssid.AAO.*target*.APPL.EXECVAR	X								
prefix.ssid.AAO.*target*.APPL.EXECBRWS	X								
prefix.ssid.AAO.*target*.APPL.IMS.AREA	X								
prefix.ssid.AAO.*target*.APPL.IMS.DATABASE	X								
prefix.ssid.AAO.*target*.APPL.IMS.DEDB	X								
prefix.ssid.AAO.*target*.APPL.IMS.ISC	X								
prefix.ssid.AAO.*target*.APPL.IMS.LINES	X								
prefix.ssid.AAO.*target*.APPL.IMS.LTERMS	X								
prefix.ssid.AAO.*target*.APPL.IMS.MSDB	X								
prefix.ssid.AAO.*target*.APPL.IMS.NODES	X								
prefix.ssid.AAO.*target*.APPL.IMS.PROGRAM	X								
prefix.ssid.AAO.*target*.APPL.IMS.REGION	X								
prefix.ssid.AAO.*target*.APPL.IMS.RTCODE	X								
prefix.ssid.AAO.*target*.APPL.IMS.STATUS	X								
prefix.ssid.AAO.*target*.APPL.IMS.TRAN	X								
prefix.ssid.AAO.*target*.APPL.MVS.ADSPACE	X								
prefix.ssid.AAO.*target*.APPL.MVS DASD	X								
prefix.ssid.AAO.*target*.APPL.MVS.ENQ	X								
prefix.ssid.AAO.*target*.APPl.MVS.OPER	X								
prefix.ssid.AAO.*target*.APPL.MVS.STATUS	X								
prefix.ssid.AAO.*target*.APPL.MVS.TAPE	X								
prefix.ssid.AAO.*target*.APPL.OSPI	X								
prefix.ssid.AAO.*target*.APPL.RULES	X								
prefix.ssid.AAO.*target*.APPL.SOF	X								

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*ssid*.AAO.*target*.APPL.TAPSHR	X								
prefix.*ssid*.AAO.*target*.APPL.TAPSREAD	X								
prefix.*ssid*.AAO.*target*.APPL.TAPSUPD	X								
prefix.*ssid*.AAO.*target*.APPL.TI	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.APPLS	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.CDRMS	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.CLSTRS	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.CDRSCS	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.LINES	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.MAJNODE	X								
prefix.*ssid*.AAO.*target*.APPL.VTAM.TERMS	X								
prefix.*ssid*.CICS.*target*.ABEND.ABEND		X							
prefix.*ssid*.CICS.*target*.AID.AID		X							
prefix.*ssid*.CICS.*target*.CLASS.CLASSES		X							
prefix.*ssid*.CICS.*target*.COMMAND.TSUT		X							
prefix.*ssid*.CICS.*target*.CONNECT.CONNECT		X							
prefix.*ssid*.CICS.*target*.CONNECT.CONNXPND		X							
prefix.*ssid*.CICS.*target*.CONNECT.CONNXPN2		X							
prefix.*ssid*.CICS.*target*.CONNECT.SESSIONS		X							
prefix.*ssid*.CICS.*target*.DB2SYSP.DB2SYSP		X							
prefix.*ssid*.CICS.*target*.DB2SYSP.DBCTL		X							
prefix.*ssid*.CICS.*target*.DB2TASK.DB2TASK		X							
prefix.*ssid*.CICS.*target*.DB2TASK.DB2TXPND		X							
prefix.*ssid*.CICS.*target*.DB2TASK.DBCTASK		X							
prefix.*ssid*.CICS.*target*.DEST.DEST		X							

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*ssid*.CICS.*target*.DLI.DLI		X							
prefix.*ssid*.CICS.*target*.DUMP.DUMP		X							
prefix.*ssid*.CICS.*target*.ENQUEUE.ENQUEUE		X							
prefix.*ssid*.CICS.*target*.EXITS.EXITS		X							
prefix.*ssid*.CICS.*target*.FILE.DATATABL		X							
prefix.*ssid*.CICS.*target*.FILE.DDIR		X							
prefix.*ssid*.CICS.*target*.FILE.DDIRXPND		X							
prefix.*ssid*.CICS.*target*.FILE.DDIRXPN2		X							
prefix.*ssid*.CICS.*target*.FILE.DSNAMES		X							
prefix.*ssid*.CICS.*target*.FILE.FILE		X							
prefix.*ssid*.CICS.*target*.FILE.FILEXPND		X							
prefix.*ssid*.CICS.*target*.FILE.FILEXPN2		X							
prefix.*ssid*.CICS.*target*.TERM.CONSOLES		X							
prefix.*ssid*.CICS.*target*.TERM.TERMINAL		X							
prefix.*ssid*.CICS.*target*.TERM.TERMXPND		X							
prefix.*ssid*.CICS.*target*.HISTORY.HISTORY		X							
prefix.*ssid*.CICS.*target*.ICE.ICE		X							
prefix.*ssid*.CICS.*target*.JOURNAL.JOURNAL		X							
prefix.*ssid*.CICS.*target*.MONITOR.MONITOR		X							
prefix.*ssid*.CICS.*target*.NUCLEUS.LPAS		X							
prefix.*ssid*.CICS.*target*.NUCLEUS.NUCLEUS		X							
prefix.*ssid*.CICS.*target*.NUCLEUS.TCBS		X							
prefix.*ssid*.CICS.*target*.PLAN.PLAN		X							
prefix.*ssid*.CICS.*target*.PLAN.PLANXPND		X							
prefix.*ssid*.CICS.*target*.PPST.PPST		X							

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*ssid*.CICS.*target*.PROBLEM.PROBLEM		X							
prefix.*ssid*.CICS.*target*.PROBLEM.CSTATUS		X							
prefix.*ssid*.CICS.*target*.PROBLEM.STATUS		X							
prefix.*ssid*.CICS.*target*.PROGRAM.PROGRAM		X							
prefix.*ssid*.CICS.*target*.PROGRAM.REMOTES		X							
prefix.*ssid*.CICS.*target*.PSB.PSBNAME		X							
prefix.*ssid*.CICS.*target*.REVIEW.REVIEW		X							
prefix.*ssid*.CICS.*target*.SHARE.SHARE		X							
prefix.*ssid*.CICS.*target*.SUBPOOL.DSAS		X							
prefix.*ssid*.CICS.*target*.SUBPOOL.SUBPOOL		X							
prefix.*ssid*.CICS.*target*.SUBPOOL.REGIONS		X							
prefix.*ssid*.CICS.*target*.SUFFIX.SUFF		X							
prefix.*ssid*.CICS.*target*.SUMMARY.SUMMARY		X							
prefix.*ssid*.CICS.*target*.TASK.MEMORY		X							
prefix.*ssid*.CICS.*target*.TASK.TASK		X							
prefix.*ssid*.CICS.*target*.TASK.TASKXPN2		X							
prefix.*ssid*.CICS.*target*.TASK.TASKXPN3		X							
prefix.*ssid*.CICS.*target*.TASK.TASKXPN4		X							
prefix.*ssid*.CICS.*target*.TASK.TASKXPND		X							
prefix.*ssid*.CICS.*target*.TEMP.TEMPSTRG		X							
prefix.*ssid*.CICS.*target*.TEMP.TEMPXPND		X							
prefix.*ssid*.CICS.*target*.TIOT.TIOT		X							
prefix.*ssid*.CICS.*target*.TRAN.TRAN		X							
prefix.*ssid*.CICS.*target*.TRAN.TRANXPND		X							
prefix.*ssid*.CICS.*target*.VTAM.VTAM		X							

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.ssid.CICS.*target*.DIAG.CONFIG		X							
prefix.ssid.CICS.*target*.DIAG.GRAFSTAT		X							
prefix.ssid.CICS.*target*.DIAG.PROGSS		X							
prefix.ssid.CICS.*target*.DIAG.QSTAT		X							
prefix.ssid.CICS.*target*.DIAG.VALIDATE		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTMAXT		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTAMXT		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM001		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM002		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM003		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM004		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM005		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM006		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM007		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM008		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM009		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTCM010		X							
prefix.ssid.CICS.*target*.ALTCLAS.ALTICV		X							
prefix.ssid.CICS.*target*.ALTCONN.ACQCONN		X							
prefix.ssid.CICS.*target*.ALTCONN.RELCONN		X							
prefix.ssid.CICS.*target*.ALTCONN.INSCONN		X							
prefix.ssid.CICS.*target*.ALTCONN.OUTCONN		X							
prefix.ssid.CICS.*target*.ALTCONN.NOTCONN		X							
prefix.ssid.CICS.*target*.ALTCONN.PURCONN		X							
prefix.ssid.CICS.*target*.ALTTERM.INSCONT		X							

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*ssid*.CICS.*target*.ALTTERM.OUTCONT		X							
prefix.*ssid*.CICS.*target*.ALTDEST.DISDEST		X							
prefix.*ssid*.CICS.*target*.ALTDEST.ENADEST		X							
prefix.*ssid*.CICS.*target*.ALTDEST.PURGETD		X							
prefix.*ssid*.CICS.*target*.ALTFILE.STADLID		X							
prefix.*ssid*.CICS.*target*.ALTFILE.STODLID		X							
prefix.*ssid*.CICS.*target*.ALTFILE.DUMDLID		X							
prefix.*ssid*.CICS.*target*.ALTDEST.RECDLID		X							
prefix.*ssid*.CICS.*target*.ALTFILE.DISFILE		X							
prefix.*ssid*.CICS.*target*.ALTFILE.ENAFILE		X							
prefix.*ssid*.CICS.*target*.ALTFILE.OPEN		X							
prefix.*ssid*.CICS.*target*.ALTFILE.CLOSE		X							
prefix.*ssid*.CICS.*target*.ALTFILE.ALLOC		X							
prefix.*ssid*.CICS.*target*.ALTFILE.FREE		X							
prefix.*ssid*.CICS.*target*.ALTICES.PURGEICE		X							
prefix.*ssid*.CICS.*target*.ALTAID.PURGEAID		X							
prefix.*ssid*.CICS.*target*.ALTTSUT.PURGETS		X							
prefix.*ssid*.CICS.*target*.ALTTERM.INSLINE		X							
prefix.*ssid*.CICS.*target*.ALTTERM.OUTLINE		X							
prefix.*ssid*.CICS.*target*.ALTCONN.AVAMODE		X							
prefix.*ssid*.CICS.*target*.ALTPROG.CICPROG		X							
prefix.*ssid*.CICS.*target*.ALTPROG.DISPROG		X							
prefix.*ssid*.CICS.*target*.ALTPROG.PGMDROP		X							
prefix.*ssid*.CICS.*target*.ALTPROG.ENAPROG		X							
prefix.*ssid*.CICS.*target*.ALTPROG.PGMLOAD		X							

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.ssid.CICS.*target*.ALTPROG.NEWCOPY		X							
prefix.ssid.CICS.*target*.ALTPROG.USEPROG		X							
prefix.ssid.CICS.*target*.ALTER.ALTERVS		X							
prefix.ssid.CICS.*target*.ALTTASK.KILL		X							
prefix.ssid.CICS.*target*.ALTTASK.KILCEMT		X							
prefix.ssid.CICS.*target*.ALTTERM.ACQTERM		X							
prefix.ssid.CICS.*target*.ALTTERM.RELTERM		X							
prefix.ssid.CICS.*target*.ALTTERM.INSTERM		X							
prefix.ssid.CICS.*target*.ALTTERM.OUTTERM		X							
prefix.ssid.CICS.*target*.ALTTRAN.CICTRAN		X							
prefix.ssid.CICS.*target*.ALTTRAN.DISTRAN		X							
prefix.ssid.CICS.*target*.ALTTRAN.ENATRAN		X							
prefix.ssid.CICS.*target*.ALTTRAN.NONTRAN		X							
prefix.ssid.CICS.*target*.ALTTRAN.PURTRAN		X							
prefix.ssid.CICS.*target*.ALTTRAN.USETRAN		X							
prefix.system.RESOLVE.ALLOCATE.UPDATE							X		X
prefix.system.RESOLVE.APF.LIST							X		X
prefix.system.RESOLVE.APF.UPDATE							X		X
prefix.system.RESOLVE.APF.EXIT							X		X
prefix.system.RESOLVE.ASM.LIST							X	X	X
prefix.system.RESOLVE.AUTHTSO.LIST							X		X
prefix.system.RESOLVE.AUTHTSO.UPDATE							X		X
prefix.system.RESOLVE.AUTHTSO.EXIT							X		X
prefix.system.RESOLVE.BBXS.LIST							X		X
prefix.system.RESOLVE.CBLOCK.LIST							X		X

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.system.RESOLVE.CDE.LIST							X		X
prefix.system.RESOLVE.CHAP.UPDATE							X		X
prefix.system.RESOLVE.CLEAR.UPDATE							X		X
prefix.system.RESOLVE.CNSL.UPDATE							X		
prefix.system.RESOLVE.COMMAND.UPDATE							X		
prefix.system.RESOLVE.CONSOLES.LIST							X		X
prefix.system.RESOLVE.CONSOLES.UPDATE							X		X
prefix.system.RESOLVE.CPU.LIST							X	X	X
prefix.system.RESOLVE.CSA.LIST							X	X	X
prefix.system.RESOLVE.CSMON.LIST							X		X
prefix.system.RESOLVE.CSMON.EXIT							X		X
prefix.system.RESOLVE.CSSUM.LIST							X		X
prefix.system.RESOLVE.DCPU.LIST							X		X
prefix.system.RESOLVE.DEALLOC.UPDATE							X		X
prefix.system.RESOLVE.DEBUG.UPDATE							X		
prefix.system.RESOLVE.DEVIATN.LIST							X		X
prefix.system.RESOLVE.DOMAIN.LIST							X		X
prefix.system.RESOLVE.DONTSWAP.UPDATE							X		X
prefix.system.RESOLVE.DSNAME.LIST							X		X
prefix.system.RESOLVE.DUMP/LIST.LIST							X		X
prefix.system.RESOLVE.DVIEW.LIST							X		X
prefix.system.RESOLVE.DVIEW.UPDATE							X		X
prefix.system.RESOLVE.EDTINFO.LIST							X		X
prefix.system.RESOLVE.ENQUEUES.LIST							X	X	X
prefix.system.RESOLVE.EQUATE.LIST							X		X

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.system.RESOLVE.ESTORAGE.LIST							X		X
prefix.system.RESOLVE.EXECUTE.UPDATE							X		X
prefix.system.RESOLVE.EXIT.UPDATE							X		X
prefix.system.RESOLVE.FCOMMON.UPDATE							X		
prefix.system.RESOLVE.FINDMBR.LIST							X		X
prefix.system.RESOLVE.HELP.LIST							X		
prefix.system.RESOLVE.INFO.LIST							X	X	X
prefix.system.RESOLVE.IO.LIST							X	X	X
prefix.system.RESOLVE.LABEL.LIST							X		X
prefix.system.RESOLVE.DVIEW.UPDATE							X		X
prefix.system.RESOLVE.LLIST.LIST							X		X
prefix.system.RESOLVE.LLIST.UPDATE							X		X
prefix.system.RESOLVE.LLIST.EXIT							X		X
prefix.system.RESOLVE.LOADLPA.UPDATE							X		X
prefix.system.RESOLVE.LOADLPA.EXIT							X		X
prefix.system.RESOLVE.LOCKS.LIST							X		X
prefix.system.RESOLVE.LOG.LIST							X		
prefix.system.RESOLVE.LPA.LIST							X		X
prefix.system.RESOLVE.LWAIT.EXIT							X		X
prefix.system.RESOLVE.MCOMMAND.UPDATE							X		X
prefix.system.RESOLVE.MDEVICE.LIST							X	X	X
prefix.system.RESOLVE.MEMSCAN.LIST							X		X
prefix.system.RESOLVE.MIO.LIST							X		X
prefix.system.RESOLVE.MLCU.LIST							X		X
prefix.system.RESOLVE.MONITOR.LIST							X	X	X

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.system.RESOLVE.MOUNT.UPDATE							X		X
prefix.system.RESOLVE.MPATH.LIST							X	X	X
prefix.system.RESOLVE.MSTORAGE.LIST							X		X
prefix.system.RESOLVE.MTP.LIST							X	X	X
prefix.system.RESOLVE.NUCLEUS.LIST							X		X
prefix.system.RESOLVE.OKSWAP.UPDATE							X		X
prefix.system.RESOLVE.PAGING.LIST							X	X	X
prefix.system.RESOLVE.PARMLIST.LIST							X		X
prefix.system.RESOLVE.PCPU.LIST							X		X
prefix.system.RESOLVE.PFKEY.LIST							X		
prefix.system.RESOLVE.PIO.LIST							X		X
prefix.system.RESOLVE.PRIVATE.LIST							X		X
prefix.system.RESOLVE.PROGRESS.LIST							X	X	X
prefix.system.RESOLVE.PRSRM.LIST							X		X
prefix.system.RESOLVE.REALLOC.UPDATE							X		
prefix.system.RESOLVE.REALTIME.UPDATE							X		
prefix.system.RESOLVE.REALTIME.LIST							X		
prefix.system.RESOLVE.REPLIES.LIST							X	X	X
prefix.system.RESOLVE.RESERVES.LIST							X	X	X
prefix.system.RESOLVE.RSM.LIST							X	X	X
prefix.system.RESOLVE.SDUMP.LIST							X		X
prefix.system.RESOLVE.SDUMP.UPDATE							X		X
prefix.system.RESOLVE.SETOP.LIST							X		X
prefix.system.RESOLVE.SMFEXIT.UPDATE							X		X
prefix.system.RESOLVE.SMFEXIT.EXIT							X		X

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.system.RESOLVE.SMSLIST.LIST							X		X
prefix.system.RESOLVE.SMSLIST.UPDATE							X		X
prefix.system.RESOLVE.SOFTFRR.LIST							X	X	X
prefix.system.RESOLVE.SPACE.LIST							X	X	X
prefix.system.RESOLVE.SRM.LIST							X		X
prefix.system.RESOLVE.SSVT.LIST							X		X
prefix.system.RESOLVE.SSVT.EXIT							X		X
prefix.system.RESOLVE.STATUS.LIST							X	X	X
prefix.system.RESOLVE.SUBMIT.UPDATE							X		
prefix.system.RESOLVE.SVCFIND.LIST							X		X
prefix.system.RESOLVE.SYSDUMP.LIST							X	X	X
prefix.system.RESOLVE.TCB.LIST							X		X
prefix.system.RESOLVE.TERM.LIST							X		X
prefix.system.RESOLVE.TIME.LIST							X		X
prefix.system.RESOLVE.TIOT.LIST							X	X	X
prefix.system.RESOLVE.TPIO.LIST							X	X	X
prefix.system.RESOLVE.TQE.LIST							X		X
prefix.system.RESOLVE.TRACK.LIST							X		
prefix.system.RESOLVE.TRTBL.LIST							X		X
prefix.system.RESOLVE.TSULIST.LIST							X	X	X
prefix.system.RESOLVE.UCB.LIST							X		X
prefix.system.RESOLVE.UNLOAD.UPDATE							X		X
prefix.system.RESOLVE.USING.LIST							X	X	X
prefix.system.RESOLVE.VIO.LIST							X		X
prefix.system.RESOLVE.VMCMD.UPDATE							X	X	X

Resource/Service name	AutoOPERATOR	MAINVIEW for CICS	MAINVIEW for DB2	MAINVIEW for MVS	MAINVIEW for DBCTL	MAINVIEW FOCAL POINT	MAINVIEW SYSPROG Services	SYSPROG from AAO	SYSPROG from MVMVS
prefix.*system*.RESOLVE.WAITING.LIST							X		X
prefix.*system*.RESOLVE.WARNING.LIST							X		X
prefix.*system*.RESOLVE.XCALL.UPDATE							X		
prefix.*system*.RESOLVE.XLOAD.LIST							X		
prefix.*system*.RESOLVE.XSERVICE.LIST							X		
prefix.*system*.RESOLVE.ZAP.UPDATE							X		X

Chapter 6. Using CLISTs to Identify Resources

BMC Software distributes several CLISTs that you can use to help identify the resources to be secured with an ESM. These CLISTs are members of the BBSAMP data set.

CLIST name	Description
RACFDEF	Defines all the product resources (listed in Table 1 on page 20) to RACF.
MIGUSER	Assists in migrating any standard BBSAMP $USERID members you might have defined with BMC Software proprietary security into RACF definitions.
AOCMDDF, AOCMDPE	Use these CLISTs to implement additional security with the CMD feature for the AutoOPERATOR product. AutoOPERATOR CMD-level resources are listed in "Resources for AutoOPERATOR Commands and Transactions: (FEATURE=CMD)" on page 49.
AOAPPLDF, AOAAPLPE	Use these CLISTs to implement additional security with the APPL feature for the AutoOPERATOR product. AutoOPERATOR APPL-level resources are listed in "Resources for AutoOPERATOR Applications: (FEATURE=APPL)" on page 44.
AOALRTDF, AOALRTPE	Use these CLISTs to implement additional security with the ALRT feature for the AutoOPERATOR product. AutoOPERATOR ALRT-level resources are listed in "Resources for AutoOPERATOR ALERTs: (FEATURE=ALRT)" on page 51.
AOEXECDF, AOEXECPE	Use these CLISTs to implement additional security with the EXEC feature for the AutoOPERATOR product. AutoOPERATOR EXEC-level resources are listed in "Resources for AutoOPERATOR EXECs: (FEATURE=EXEC)" on page 51.
AOPARMDF, AOPARMPE	Use these CLISTs to implement additional security with the PARM feature for the AutoOPERATOR product. AutoOPERATOR PARM-level resources are listed in "Resources for AutoOPERATOR Parameter Data: (FEATURE=PARM)" on page 52.
CICSRACF	Use this CLIST to define all CICS resources to RACF.
DB2CMDDF, DB2CMDPE	Use these CLISTs to implement additional security with the CMD feature for the MAINVIEW for DB2 product. CMD-level resources are listed in "Resources for MAINVIEW for DB2" on page 62.

Creating Resource Names for MAINVIEW Products

Use the RACFDEF CLIST to identify the resources listed in Table 1 on page 20 to RACF.

The RACFDEF CLIST prompts you to enter the

- prefix to use as the high-level qualifier for each resource
- security class to use ($BOOLE)
- SSID of the BBI-SS PAS you are securing
- default access rights for all resources: UACC(READ) or UACC(NONE)
- target you are securing (targets must be existing targets in the BBPARM member BBIJNT00)

Run this CLIST once for every BBI-SS PAS and for every target you are securing.

Migrating Existing Resource Names for MAINVIEW Products

Use the MIGUSER CLIST to migrate any security you may have defined in BBPARM member $USERID with BMC Software proprietary security. The definitions in $USERID must be syntactically correct for this CLIST to run successfully.

The $USERID member should not include any generic AUTHJOB definitions unless the security class defined has been implemented as a generic class. The value specified in the AUTHJOB keyword is equivalent to the *target* node of the resource name.

The MIGUSER CLIST prompts you to enter a

- SSID of the BBI-SS PAS you are securing
- prefix to use as the high-level qualifier for each resource
- security class to use ($BOOLE)
- user ID to migrate
- name of the BBPARM data set member that you are trying to convert (do not specify quotation marks in the data set name)

Creating Resource Names for AutoOPERATOR

AutoOPERATOR product security can be implemented with up to five additional features, as described in "Resources for AutoOPERATOR: Advanced Security" on page 42. If you plan to implement security for any of these features, you must complete the instructions in Chapter 7, "Activating Basic Security".

Use the CLISTs described in Table 10 to help identify the resources associated with each additional feature. Each CLIST prompts you to enter the

- security class to use ($BOOLE)
- prefix to use as the high-level qualifier for each resource
- SSID of the BBI-SS PAS you are securing
- default access rights for all resources: UACC(READ) or UACC(NONE)
- target you are securing (targets must be existing targets in the BBPARM member BBIJNT00)

If you choose to modify any CLIST, make a copy of it first.

Run each CLIST once for every BBI-SS PAS and for every target you are securing.

Table 10. AutoOPERATOR Security CLISTs

Feature	Secures	CLIST	Function
FEATURE=CMD	CICS transactions, IMS transactions, IMS commands, and MVS commands from an AutoOPERATOR 3.1 terminal session. See page 49 for a list of CMD-level resource names.	AOCMDDF	Identifies the resources to be secured to RACF.
		AOCMDPE	Helps you permit access to the secured resources.
FEATURE=APPL	Access to AutoOPERATOR applications in a BBSEC member. See page 44 for a list of APPL-level resources and names.	AOAPPLDF	Identifies the resources to be secured to RACF.
		AOAPPLPE	Helps you permit access to the secured resources.
FEATURE=ALRT	ALERTs and ALERT queues from deletion in the AutoOPERATOR ALERT Display and AutoOPERATOR ALERT Detail applications. See page 51 for a list of ALRT-level resources and names.	AOALRTDF	Identifies the resources to be secured to RACF.
		AOALRTPE	Helps you permit access to the secured resources.
FEATURE=EXEC	Individual EXECs from scheduling by EXEC name. See page 51 for a list of EXEC-level resources and names.	AOEXECDF	Identifies the resources to be secured to RACF.
		AOEXECPE	Helps you permit access to the secured resources.
FEATURE=PARM	Parameter members from being updated, read, added, deleted, or activated in the AutoOPERATOR Dynamic Parameter Manager application. See page 52 for a list of PARM-level resources and names.	AOPARMDF	Identifies the resources to be secured to RACF.
		AOPARMPE	Helps you permit access to the secured resources.

Creating Resource Names for CICS Resources

Use this CLIST to implement additional security with the CICS feature for the MAINVIEW for CICS (Release 3.4.1) product and the AutoOPERATOR for CICS option. By choosing the CICS feature, you are securing the use of CICS action, display, and diagnostic services.

The CICSRACF CLIST identifies the CICS resources to be secured to RACF and prompts you to enter the

- prefix to use as the high-level qualifier for each resource
- security class to use ($BOOLE)
- SSID of the BBI-SS PAS you are securing
- default access rights for all resources: UACC(READ) or UACC(NONE)
- type, which determines which security definitions are generated
- delete option, which determines whether to add or delete definitions generated
- target you are securing (targets must be existing targets in the BBPARM member BBIJNT00)

Run this CLIST once for every BBI-SS PAS and for every target you are securing.

Important

If you plan to implement security for CICS resources, you must complete the instructions in Chapter 7, “Activating Basic Security”.

Creating Resource Names for MAINVIEW for DB2 CMD-Level Security: DB2CMDDF and DB2CMDPE

Use these CLISTs to implement additional security with the CMD feature for the MAINVIEW for DB2 (Release 5.1 and above) product. By choosing the CMD feature, you are securing use of DB2 commands from a terminal session.

CMD-level resource names are listed in "Resources for MAINVIEW for DB2" on page 62. If you need to modify these CLISTs, you should change a copied version.

BBSAMP contains the DB2CMDDF CLIST to help you identify the resources to be secured to RACF and prompts you to enter the

- security class to use ($BOOLE)
- prefix to use as the high-level qualifier for each resource
- SSID of the BBI-SS PAS you are securing
- default access rights for all resources: UACC(READ) or UACC(NONE)
- target you are securing (targets must be existing targets in the BBPARM member BBIJNT00)
- command and operand to be secured

Run this CLIST once for every BBI-SS PAS and for every target you are securing.

The DB2CMDPE CLIST helps you permit access to the secured resources for a specific user and prompts you to enter the

- security class to use ($BOOLE)
- prefix to use as the high-level qualifier for each resource
- SSID of the BBI-SS PAS to which you are permitting access
- target to which you are permitting access (targets must be existing targets in the BBPARM member BBIJNT00)
- resources to which you are permitting access

Run this CLIST once for every BBI-SS PAS and user being permitted access.

Important

If you plan to implement CMD-level security, you must complete the instructions in Chapter 7, "Activating Basic Security".

Chapter 7. Activating Basic Security

This chapter explains how to create and update the BBSEC member and add it to SYS1.PARMLIB to activate security. This chapter assumes you have

- identified which product resources you want to secure as described in Chapter 4, "Reviewing Product Resources" on page 17
- defined the resources to your ESM and granted or denied access to them as described in Chapter 5, "Configuring Your ESM for Basic Security" on page 65

Creating the Basic Security Member BBSEC

Basic security for the following MAINVIEW products is controlled by the presence of control statements in the SYS1.PARMLIB member BBSEC:

AutoOPERATOR
InTune
MAINVIEW for DBCTL
MAINVIEW for CICS
MAINVIEW for IMS
MAINVIEW for DB2
MAINVIEW FOCAL POINT
MAINVIEW SYSPROG Services
COMMON STORAGE MONITOR

Note: For MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR, BBSEC can reside in any data set included in the logical parmlib concatenation. See "Adding BBSEC to BBPARM and SYS1.PARMLIB" on page 97 for additional information.

To create a BBSEC member:

1. Create a PDS member called BBSEC in a working data set or your personal data set.

   Important! Do not add BBSEC to SYS1.PARMLIB until you are ready to activate security. Once you have completed the member and want to activate security, you will copy BBSEC to BBPARM or SYS1.PARMLIB, as described on page 97.

2. Basic security for a product or group of products is activated by the TYPE statement in BBSEC. The format of the TYPE statement is described in "BBSEC TYPE= Statement" on page 92.

   Use an editor to add as many TYPE statements as necessary to activate security for your products. Save your changes.

3. When you are ready to activate security, see "Adding BBSEC to BBPARM and SYS1.PARMLIB" on page 97.

4. Consider protecting the data set containing BBSEC from unauthorized modification.

BBSEC Syntax

Observe the following syntax when updating BBSEC:

- Each TYPE statement and its parameters can be specified in positions 1–72 on one or more lines, as shown in Figure 3
- Enter keywords in the format `keyword=value` (for example, `TYPE=BBI`)
- Indicate comment lines with an asterisk (*) in column 1
- To continue a TYPE statement on the next line, put a comma at the end of the line to be continued
- Do not break multivalue keywords across lines

  For example, `FEATURE=(CMD,APPL,EXEC)` must appear on the same line.

A sample BBSEC member is shown here:

```
* Activates security for common resources:
*
TYPE=BBI,SS=SJSB,PREFIX=BBM,CLASS=$BOOLE
*
* Activates security for SYSPROG and CSMON services:
*
TYPE=SYSPROG,
AUDIT=FAILED,
TRACE=NO, INIT=YES
```

Figure 3. Sample BBSEC Member

BBSEC TYPE= Statement

The format of the TYPE statement for MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR services is

```
TYPE=SYSPROG,PREFIX=prefix,CLASS=class,ACTION=[DISABLE|ENABLE],
          AUDIT=[NONE|ALL|UPDATE|FAILED|BOTH],
          TRACE=[YES|NO],WARN=[YES|NO],INIT=[YES|NO],
          ERRPROC=[FAIL|ALLOW],AUDRTE=(9),AUDDSC=(4),
          SYSID=[SMF|CVT],USECNNM=[YES|NO]
```

The format of the TYPE statement for AutoOPERATOR advanced security and MAINVIEW for DB2 command-level security is

```
TYPE=product,SSID=ssid,PREFIX=prefix,CLASS=class,
          FEATURE=(feature,feature,feature)
```

The format of the TYPE statement for all other products is

```
TYPE=product,SSID=ssid,PREFIX=prefix,CLASS=class
```

The TYPE statement parameters are

Parameter	Explanation
TYPE=*product*	Activates security for the specified product or group of products. Specify one of the following products on each TYPE statement. Specify as many TYPE statements as needed. BBI — Activates security for the resources that are common to the following products, as described on page 19: AutoOPERATOR MAINVIEW for CICS MAINVIEW for DB2 MAINVIEW for DBCTL MAINVIEW for IMS MAINVIEW FOCAL POINT AAO — Activates additional security for AutoOPERATOR commands, applications, EXECs, ALERTs, and parameter data as described in "Resources for AutoOPERATOR: Advanced Security" on page 42. **A TYPE=BBI statement must also be specified.** CICS — Activates additional security for the resources described in "Resources Common to MAINVIEW for CICS and the AutoOPERATOR for CICS Option" on page 35. **A TYPE=BBI statement must also be specified.** DB2 — Activates additional security for the resources described in "Resources for MAINVIEW for DB2" on page 62. **A TYPE=BBI statement must also be specified.** INTUNE — Activates security for the resources described in "Resources for InTune" on page 63. SYPROG — Activates security for the resources described in "Resources Common to MAINVIEW SYSPROG Services, AutoOPERATOR, and MAINVIEW for MVS" on page 24. Either TYPE=SYSPROG or TYPE=RESOLVE may be specified.
SSID=*ssid* or SS=*ssid*	**Not for TYPE=SYSPROG.** Is the one- to four-character BBI-SS PAS name where resources are to be protected. The SSID is part of the resource name used to define resources to your ESM. Each SSID used in a resource name must be specified on a separate TYPE statement in BBSEC. For example, if you have defined resources names to your ESM that included SSIDs of SYS1, SYS2, SYS3, and SYS4, you must specify a TYPE statement for each of these SSIDs. Refer to "BBSEC Examples" on page 95 for examples. **Note:** Although an asterisk (*) can be used as a wildcard for the `SSID` value and activates security for all BBI-SS PASs, it is not recommended.

Parameter	Explanation (Continued)
PREFIX= *prefix*	Is the one- to eight-character prefix for all resource names. The default prefix is BBM. Specify the prefix that you used in the resource names when defining resources to your ESM.
CLASS=*class*	For TYPE=INTUNE, specify CLASS=DATASET. For all other products, CLASS is the optional one- to eight-character security class name used to identify your MAINVIEW product resources. The default security class is $BOOLE. This security class must be defined to your ESM as described in Chapter 5, "Configuring Your ESM for Basic Security".
FEATURE=(CMD) FEATURE=(CMD,APPL, EXEC,ALRT,PARM)	For TYPE=DB2, specify: CMD for DB2 command-level security For TYPE=AAO, specify one or more of the following values: CMD AutoOPERATOR command and parameter security APPL AutoOPERATOR application security EXEC AutoOPERATOR individual EXEC authority ALRT AutoOPERATOR ALERTs authority PARM AutoOPERATOR parameter The FEATURE parameter and its keywords must be specified on a single line in BBSEC. Separate mulitple keywords by a comma, as shown at left. Enclose keywords in parentheses.
ACTION=[ENABLE| DISABLE]	**For TYPE=SYSPROG only.** Indicates whether security should be enabled or disabled. Specify DISABLE only to disable security calls due to a problem. The default is ENABLE.
AUDIT=[NONE|ALL| UPDATE|FAILED| BOTH]	**For TYPE=SYSPROG only.** Determines if, and to what extent, auditing of service requests should be performed. Audit messages are displayed according to the descriptor and routing codes you have specified. The parameter values are as follows: NONE (Default.) No audit messages are produced. ALL An audit message is produced for every security request. UPDATE Audit messages are produced for all security requests except those containing a function of LIST in the entity string, regardless of the result. FAILED An audit message is produced when the security system denies access. BOTH An audit message is produced when the criteria for either FAILED or UPDATE is met.

Parameter	Explanation (Continued)
AUDDSC=(4)	**For TYPE=SYSPROG only.** Specifies the descriptor codes for audit and trace messages. Specify one or more codes separated by commas and enclosed in parentheses. The default is AUDDSC=(4).
AUDRTE=(9)	**For TYPE=SYSPROG only.** Specifies the route codes for audit and trace messages. Specify one or more route codes separated by commas and enclosed in parentheses. The default is AUDRTE=(9).
ERRPROC=[FAIL|ALLOW]	**For TYPE=SYSPROG only.** Indicates how requests should be handled if the security system is not accessible. ERRPROC=FAIL indicates that all requests should be denied when the security system is not accessible. ERRPROC=ALLOW indicates that all requests should be allowed. The default is ERRPROC=FAIL.
INIT=[YES|NO]	**For TYPE=SYSPROG only.** Indicates whether a security call should be issued during initialization to determine if initialization should be allowed to continue. The default is INIT=NO.
SYSID=[SMF|CVT]	**For TYPE=SYSPROG only.** Indicates the source of the system identifier. If SYSID=SMF is specified, the SMF identifier in field SMCASID is used. If SYSID=CVT is specified, the value in CVTSNAME is used. If CVTSNAME does contain a value, the identifier in SMCASID is used. The default is SYSID=CVT.
TRACE=[YES|NO]	**For TYPE=SYSPROG only.** Indicates whether a message containing the parameters for each security request is issued. The default is TRACE=NO.
USECNNM=[YES|NO]	**For TYPE=SYSPROG only.** USECNNM=YES causes SYSPROG to use the console name for security verification. USECNNM=NO causes SYSPROG to use its address space authority for security checks. The default is USECNNM=YES.
WARN=[YES|NO]	**For TYPE=SYSPROG only.** Indicates whether a request should be allowed even though the security system denied access. WARN=YES allows you to test security without denying access. The default is WARN=NO.

BBSEC Examples

To use the default prefix BBM for the resources and identify them to the default security class $BOOLE, BBSEC might contain the following lines:

```
* The following turns on security for BBI-SS PAS SYS1, SYS2,
* SYS3, and SYS4 to security class $BOOLE

TYPE=BBI,SS=SYS1
TYPE=BBI,SS=SYS2
TYPE=BBI,SS=SYS3
TYPE=BBI,SS=SYS4
```

To use a prefix of CHARLIE for the resources and identify them to a security class of SECURE for multiple BBI-SS PASs with different SSID names, BBSEC might contain the following lines:

```
* The following turns on security for BBI-SS PAS SYS1, SYS2,
* SYS3, and SYS4 to security class SECURE

TYPE=BBI,SS=SYS1,PREFIX=CHARLIE,CLASS=SECURE
TYPE=BBI,SS=SYS2,PREFIX=CHARLIE,CLASS=SECURE
TYPE=BBI,SS=SYS3,PREFIX=CHARLIE,CLASS=SECURE
TYPE=BBI,SS=SYS4,PREFIX=CHARLIE,CLASS=SECURE
```

To secure the CMD and APPL features of AutoOPERATOR, define them as follows:

```
* The following turns on security for BBI-SS PAS SYS1, to
* security class $BOOLE

TYPE=BBI,SS=SYS1,CLASS=$BOOLE

* The following turns on security for the CMD and the APPL
* features of AutoOPERATOR security

TYPE=AAO,SSID=SYS1,FEATURE=(CMD,APPL)
```

The following example of BBSEC secures the AutoOPERATOR CMD feature for multiple BBI-SS PASs with different SSIDs:

```
* The following turns on security for BBI-SS PAS SYS1, SYS2,
* SYS3, and SYS4

TYPE=BBI,SS=SYS1
TYPE=BBI,SS=SYS2
TYPE=BBI,SS=SYS3
TYPE=BBI,SS=SYS4

* The following turns on security for the CMD feature of AutoOPERATOR
* advanced security for BBI-SS PASs SYS1, SYS2, SYS3, and SYS4

TYPE=AAO,SS=SYS1,FEATURE=(CMD)
TYPE=AAO,SS=SYS2,FEATURE=(CMD)
TYPE=AAO,SS=SYS3,FEATURE=(CMD)
TYPE=AAO,SS=SYS4,FEATURE=(CMD)
```

The following example of BBSEC activates security for the MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR services:

```
*
* Activates security for SYSPROG and CSMON services:
*
TYPE=SYSPROG,
AUDIT=FAILED,
TRACE=NO, INIT=YES
```

Adding BBSEC to BBPARM and SYS1.PARMLIB

Use the following procedure for AutoOPERATOR, MAINVIEW for DBCTL, MAINVIEW for CICS, MAINVIEW for IMS, MAINVIEW for DB2, and MAINVIEW FOCAL POINT.

1. After you have updated BBSEC to include the appropriate TYPE statements, copy BBSEC to the BBPARM data set before you copy it to SYS1.PARMLIB. This process will minimize the impact of activating security: only those BBI-SS PASs that reference the BBPARM data set will be affected.
2. Warm start each BBI-SS PAS for the member to take effect.
3. Test and fine tune security at the BBI-SS PAS level before activating security for your entire system.
4. Once you are satisfied with the way security is working at the BBI-SS PAS level, copy BBSEC to SYS1.PARMLIB. The BBSEC member in SYS1.PARMLIB overrides any BBSEC members in the BBPARM data set.

For MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR, BBSEC is processed by program BBXSAF00. BBXSAF00 obtains BBSEC from the OS/390 logical parmlib concatenation (available in OS/390 version 1 release 2 and later) during OS/390 system initialization. Therefore, BBSEC can reside in any data set that is included in the logical parmlib concatenation: it does not have to be in SYS1.PARMLIB. If you change the BBSEC member in the logical parmlib concatenation and you want that change to become effective before the OS/390 system is restarted, you can execute program BBXSAF00, as described on page 99. Use the following procedure to activate BBSEC:

1. After you have updated BBSEC to include the appropriate TYPE=SYSPROG (or TYPE=RESOLVE) statements, copy BBSEC to a data set in the logical parmlib concatenation.
2. Wait for the OS/390 system to be restarted, or execute program BBXSAF00, as described in “Activating Changes to BBSEC by Executing BBXSAF00” on page 99.

Disabling Basic Security

To disable basic security for AutoOPERATOR, MAINVIEW for DBCTL, MAINVIEW for CICS, MAINVIEW for IMS, MAINVIEW for DB2, or MAINVIEW FOCAL POINT, perform the following steps:

1. In the BBSEC member in both the BBPARM data set and in SYS1.PARMLIB, change the appropriate TYPE= statements to comments by typing an asterisk in column one of the TYPE statement.
2. Warm start each affected BBI-SS PAS.

To disable basic security for all products:

1. Remove the BBSEC member from both the BBPARM data set and SYS1.PARMLIB, or rename BBSEC.
2. Warm start each affected BBI-SS PAS.

To disable basic security for MAINVIEW SYSPROG Services and COMMON STORAGE MONITOR, perform the following steps:

1. Update any TYPE=SYSPROG (or TYPE=RESOLVE) statements in the BBSEC member in both the BBPARM data set and in the logical parmlib concatenation data set to specify ACTION=DISABLE.
2. Wait for the OS/390 system to be restarted, or execute program BBXSAF00, as described in "Activating Changes to BBSEC by Executing BBXSAF00" on page 99.

Chapter 8. Securing SYSPROG and CSMON Services

To secure MAINVIEW SYSPROG Services and Common Storage Monitor services, you define rules, permits, or profiles to control access to the services, as described in Chapter 5, "Configuring Your ESM for Basic Security". The resource names for the services are described in Chapter 4, "Reviewing Product Resources". You then add the TYPE=SYRPROG statement to the BBSEC security member, as described in Chapter 7, "Activating Basic Security".

This chapter explains how to

- execute BBXSAF00 to activate changes to the BBSEC security member
- review or override the default *function* qualifier used in the resource name for each SYSPROG service
- use an exit to change the *function* qualifier in a resource name for a service to anything you like

Activating Changes to BBSEC by Executing BBXSAF00

The BBSEC member contains security parameters and is used to activate basic security (see Chapter 7, "Activating Basic Security" for details). For MAINVIEW SYSPROG Services and Common Storage Monitor services, the BBSEC member is obtained from the OS/390 system logical parmlib concatenation (available in OS/390 version 1 release 2 and later). If you change BBSEC for MAINVIEW SYSPROG Services and Common Storage Monitor services and you want that change to become effective before the OS/390 system is restarted, you can execute program BBXSAF00 at any time.

Note: Do not run BBXSINIT to activate your changes. Doing so wastes common storage and may adversely affect MAINVIEW products.

Use the sample JCL shown in Figure 4 to execute BBXSAF00. Replace `hilevel.BBLINK` with the name of the data set that contains BBXSAF00.

```
//BBSEC EXECPGM=BBXSAF00,PARM=REFRESH
//STEPLIB  DD DISP=SHR,DSN=hilevel.BBLINK
//SAFCRPT  DD SYSOUT=*
//
```

Figure 4. Sample Job for Executing BBXSAF00

Consider protecting BBXSAF00 and the data set that contains BBSEC from unauthorized access.

Determining the Function Qualifier for SYSPROG Resource Names

All SYSPROG service resource names end with a function qualifer. You can determine the default function qualifier used in the resource name for each SYSPROG service in one of two ways:

- Use the XSERVICE service to display information about the service. To do so, enter `XS,`*service*, where *service* is the name of the service you are interested in.
- Browse the service name table, which is distributed as member ASTXA1SN in the BBSRC data set.

You can use the service name table to review or override the default function qualifier used in the resource name for each SYSPROG service. The service name table associates a service name to a corresponding load module name and defines attributes for the service.

Each service is defined with a ASTSNAME macro in the service name table. For example, the ASTSNAME macro for the ALLOCATE service is

ASTSNAME ALLOCATE,A1,OPER=YES,FUNCTION=UPDATE

The FUNCTION parameter specifies the function qualifier that is to be appended to the resource name passed to the ESM. The FUNCTION can be one of the following keywords:

LIST Indicates the function displays data.

UPDATE Indicates the function updates data.

EXIT Indicates that an exit routine for the service is called to determine the *function* qualifier. Certain SYSPROG services use BMC-provided exit routines. You may write your own exit, as described in "Using an Exit to Modify the Function Qualifier in SYSPROG Resource Names".

For a description of the other ASTSNAME macro parameters, see the ASTX1SN member itself.

Using an Exit to Modify the Function Qualifier in SYSPROG Resource Names

All SYSPROG service resource names end with a function qualifer of LIST or UPDATE. However, you can write an exit routine to set the function qualifier to any value you like.

When FUNCTION=EXIT is specified on the service's ASTSNAME statement in ASTXA1SN, SYSPROG attempts to call an exit routine. The exit name is ASTSEC*xx*, where *xx* is the two character module ID specified as the second positional parameter in the ASTSNAME macro.

If the exit routine exists, it executes and examines the parameters specified on the service request to determine the appropriate qualifier. If the exit routine does not exist, the qualifier is set to UPDATE.

The function qualifier cannot exceed seven characters.

Exit routines are supplied for services that have both LIST and UPDATE functions. The source for these exit routines may be found in BBSRC and used as a model for creating your own exit for a service.

Determining the Function Qualifier for CSMON Resource Names

The function qualifiers for CSMON services are shown in Table 11.

Table 11. CSMON *function* Qualifiers

Service	***function* Qualifier**
OVERVIEW	LIST
SUMMARY	LIST
STATUS	LIST
DISPLAY	LIST
ALTER	UPDATE
FREE	UPDATE

CSMON services are not defined in the ASTXA1SN service name table and cannot be modified with a user routine.

Using the Password Utility

BMC Software strongly suggests that you implement the basic security SAF interface instead of using the password utility for MAINVIEW SYSPROG Services.

However, the password utility is provided for those customers who do not have an ESM. The password utility is called after the SAF interface is called.

To restrict access to a service, you assign a password to the service by submitting a batch job. The JCL and control statements are explained in "Password Utility JCL" on page 102.

When a user requests a password-protected service, the following message is issued:

`AMT00AA ENTER PASSWORD FOR SERVICE` *service-name*

If the correct password is entered in response to the message, the service is invoked. If an incorrect password is entered, access is denied and the following message is issued:

```
AMT00BI PASSWORD INVALID, REQUEST IGNORED
```

The user must request the service again.

Password Utility JCL

To add, change, or delete passwords for one or more services, use the sample JCL shown in Figure 5.

```
//SECURITY  JOB     ACCT
//SECURITY  EXEC    PGM=ASTXA1SC
//STEPLIB   DD      DISP=SHR,DSN=hilevel.BBLINK
//SYSPRINT  DD      SYSOUT=A
//LOAD      DD      DISP=SHR,DSN=hilevel.BBLINK
//SYSIN     DD      *
//SYSIN DD *
```

Figure 5. Password Utility JCL

Substitute your load library for `hilevel.BBLINK.`

Specify the control statements on the `SYSIN DD` statement according to these rules:

- To **add** a password, use this syntax:

  service_name,,new_password

  For example, `ENQ,,NEWPASS` establishes the password NEWPASS for the ENQ service.

- To **change** a password, use this syntax:

  service_name,old_password,new_password

  For example, `ENQ,NEWPASS,NEWRPASS` changes ENQ's password from NEWPASS to NEWRPASS.

- To **delete** a password, use this syntax:

  service_name,old_password

  For example, `ENQ,NEWRPASS` removes password protection for the ENQ service.

- Begin each *service_name* in column 1.

- Specify *service_name* as the complete name of the service or as a shorter version that qualifies as a unique identifier. For example, the *service_name* for ENQUEUES could be ENQUEUES, ENQUE, ENQ, or EN, all of which are unique.

Example: The control statements in Figure 6 on page 103 specify the following changes:

- Establish a new password, NEWPASS, for the ENQ service

- Replace the old password, OLDAPF, with the new password, NEWAPF, for the APF service

- Delete the password ZAPPASS from the ZAP service

```
//SYSIN DD *
ENQ,,NEWPASS
APF,OLDAPF,NEWAPF
ZAP,ZAPPASS
/*
```

Figure 6. Sample Password Utility Control Statements

The SYSIN statements shown in Figure 6 produces the output shown in Figure 7.

```
AMTPW00I  ---SYSPROG, PASSWORD MAINTENANCE UTILITY---

AMTPW10I  APF,********,********
AMTPW20I  OLD PASSWORD SUCCESSFULLY DELETED
AMTPW30I  NEW PASSWORD SUCCESSFULLY ADDED

AMTPW10I  ENQ,,*******
AMTPW30I  NEW PASSWORD SUCCESSFULLY ADDED

AMTPW05I  ZAP,*******
AMTPW20I  OLD PASSWORD SUCCESSFULLY DELETED

AMTPW90I  PASSWORD MAINTENANCE COMPLETE - HIGHEST RETURN CODE WAS
00
```

Figure 7. Sample Password Utility Output

Password Utility Return Codes

The password utility return codes are as follows:

00 All requested functions completed without error
04 One or more functions completed with warnings
08 One or more functions terminated because of control statement syntax errors
12 One or more functions failed to complete successfully
16 Processing terminated prematurely

Part 3. Enhanced Security

This part describes enhanced security and the steps for providing enhanced security to protect your product's resources.

Chapter 9. Introduction to Enhanced Security 109
Which Products Use Enhanced Security? 109
How Enhanced Security Works 110
Authorization at the CAS, PAS, and TS User Levels 110
MAINVIEW Resources 111
Resource Naming Convention 111
Finding Entity Names 113
Exploiting the Resource Naming Convention 113
Security Parameter Library 115
Sharing a Security Parameter Library Between CASs 115
Views for Administering Enhanced Security 116
Using Security Views to Change Resource Attributes 117
Establishing Enhanced Security 119
Disabling Enhanced Security for All MAINVIEW Resources 120
Determining Which Security Members Are Active 121
CAS Security Members 121
PAS Security Member 122

Chapter 10. Configuring Your ESM for Enhanced Security 123
Configuring CA-ACF2 123
Step 1: Setting the Required GSO Record Options 124
Step 2: Authorizing the PAS and CAS 124
Step 3: Updating the CA-ACF2 SAFDEF List 126
Step 4: (Optional) Adding a SAF Resource Class to CA-ACF2 127
Step 5: (Optional) Defining Rules for Controlling View Resources 129
Configuring RACF 132
Step 1: Authorizing the CAS and PAS 132
Step 2: (Optional) Adding Resource Classes to RACF 133
Step 3: Creating RACF Security Profiles 135
Step 4: Specifying Profiles to Control Access to Product Resources 136
Configuring CA-TOP SECRET 138
Step 1: Defining a New CA-TOP SECRET Facility Matrix Entry 139
Step 2: Authorizing the CAS and PAS 140
Step 3: (Optional) Adding a New SAF Resource Class 141
Step 4: Defining Ownership of Resources 142
Step 5: Controlling Access to Product Resources 143

Chapter 11. Class Definitions 145
Working with Class Definition Members 145
Displaying a List of Class Definition Members (SECDEFL) 145
Creating a Class Definition Member 146
Activating a New Class Definition Member 147
Deleting a Class Definition Member 147
Working with Class Definitions 147
Displaying a Class (SECDEF) 147
Changing a Class 149
Adding a New Class 151
Deleting a Class 152

Recovering a Deleted Class 152
Dynamically Activating Class Changes 152

Chapter 12. Parameter Definitions 155
Displaying a List of Parameter Definitions (SEPDEFL) 156
Displaying a Parameter Definition (SEPDEF and SEPDEFD) 156
Changing a Parameter Definition 157
Creating a New Parameter Definition 160
Activating a Parameter Definition 161
Deleting a Parameter Definition 161

Chapter 13. Resource Definitions 163
Before You Begin 163
Working with Resource Definition Members 164
Displaying a List of Members using the SERDEFL View 164
Creating a New Resource Definition Member 164
Activating a New Member for Common Resources 165
Activating a New Member for Product Resources 165
Deleting a Member 166
Working with Resource Definitions 167
Browsing a Resource Definition 168
Enabling a Resource Definition 169
Disabling a Resource Definition 169
Changing a Resource Definition 169
Canceling Resource Definition Changes 171
Saving a Resource Definition 171

Chapter 14. Protecting the MAINVIEW Security Interface 173

Chapter 15. Resources Definitions Listed by Product 175
Common MAINVIEW Resources 175
Plex Manager Resources 183
CMF MONITOR and MAINVIEW for OS/390 Resources 193
MAINVIEW Alarm Manager Resources 209
MAINVIEW for CICS Resources 212
MAINVIEW for DATA ACCELERATOR Compression 215
MAINVIEW for DB2 Resources 217
MAINVIEW Explorer 220
MAINVIEW for IMS Resources 221
MAINVIEW for IP Resources 225
MAINVIEW for MQSeries Resources 226
MAINVIEW SYSPROG Services Resources 251
MAINVIEW for UNIX System Services Resources 255
MAINVIEW VistaPoint Resources 259
MAINVIEW for VTAM Resources 261
MAINVIEW for WebSphere Resources 263

Chapter 16. Resource Definitions Listed by View 265
Common Views 265
Plex Manager Views 266
CMF MONITOR and MAINVIEW for OS/390 Views 267
MAINVIEW Alarm Manager Views 275
MAINVIEW for CICS Views 276
MAINVIEW for DATA ACCELERATOR Compression Views 280

MAINVIEW for DB2 Views 281
MAINVIEW Explorer Views 282
MAINVIEW for IMS Views 283
MAINVIEW for IP Views 288
MAINVIEW for MQSeries Views 290
MAINVIEW SYSPROG Services Views 292
MAINVIEW for UNIX System Services Views 293
MAINVIEW VistaPoint Views 297
MAINVIEW for VTAM Views 298
MAINVIEW for WebSphere Views 300

Chapter 9. Introduction to Enhanced Security

This chapter provides information about the following topics:

- which products use enhanced security
- how enhanced security works
- authorization at the CAS, PAS, and TS user (UAS) levels
- MAINVIEW resources
- views for administering enhanced security
- security parameter library
- establishing enhanced security
- disabling enhanced security
- determining which security members are active

Note: The information in this chapter does not apply to MAINVIEW Alternate Access. To implement MAINVIEW Alternate Access security, see "Defining Security for MAINVIEW Alternate Access" on page 305.

Which Products Use Enhanced Security?

The following products operate either partially or completely in windows mode. When operating in windows mode, they use enhanced security:

- CMF MONITOR
- MAINVIEW Alarm Manager
- MAINVIEW for CICS
- MAINVIEW for DATA ACCELERATOR Compression
- MAINVIEW for DB2
- MAINVIEW for DBCTL
- MAINVIEW Explorer
- MAINVIEW for IMS
- MAINVIEW for IP
- MAINVIEW for MQSeries (formerly known as Command MQ for S/390)
- MAINVIEW for OS/390
- MAINVIEW SYSPROG Services
- MAINVIEW for UNIX System Services
- MAINVIEW VistaPoint
- MAINVIEW for VTAM
- MAINVIEW for WebSphere
- Plex Manager

Some of these products also operate in full-screen mode and, therefore, also use basic security. See Chapter 3, "Introduction to Basic Security" for more information on basic security.

Enhanced security is **enabled** for all of these products when they are shipped. If you want to disable security completely, see "Disabling Enhanced Security for All MAINVIEW Resources" on page 120.

How Enhanced Security Works

Like any security interface, enhanced security does not actually protect resources. Instead, it identifies MAINVIEW resources to your ESM and asks if a user is authorized to access the resource, as described here:

1. MAINVIEW resources are identified to the ESM using a class name and entity names. There are hundreds of resources, however, they can all be identified by 13 resource definitions.
2. A MAINVIEW user requests access to a protected resource. The MAINVIEW product passes the resource class name and entity name to the MAINVIEW security interface.
3. The MAINVIEW security interface passes the class name and entity name to the MVS System Authorization Facility (SAF).
4. SAF passes the request to your ESM, conceptually asking the ESM “Can this user access this resource under these circumstances?”
5. The ESM checks the user ID against the existing permit, profile, or rule (depending on the ESM) that protects the resource.
6. The ESM responds to the question with yes, no, or maybe, which it relays through SAF to the MAINVIEW security interface.
7. The MAINVIEW security interface relays the ESM’s response, permitting or denying user access to the resource, to the MAINVIEW product, display, or action.

Authorization at the CAS, PAS, and TS User Levels

Access authorization requests are made to the ESM at the CAS, PAS, and TS user levels, as described here.

- CAS
  The coordinating address space (CAS) provides all communication between a terminal session (TS) and an address space where a product runs (PAS) and other CASs running on local and remote systems. Plex Manager, shipped with all MAINVIEW products, runs in the CAS. Other products, like MAINVIEW VistaPoint, may run in a CAS. The CAS itself requires ESM authorization to access certain resources before it can initialize.

  Each time a CAS starts, non-modifiable CAS subsystem intialization authorization requests may be made to

  – verify that the user ID associated with the CAS started task has the authority to define the specified MVS subsystem ID (create the MVS SSCT)

  – determine if the address space has the authority to initialize the MVS subsystem (activate and use the specified MVS SSCT)

  – determine if the address space can initialize without any MAINVIEW security

- PAS
  Each product runs in a product address space (PAS). The address space where the product is running requires ESM authorization to common and product resources managed by MAINVIEW enhanced security. After successful CAS initialization, authorization

requests are made when a product attempts to connect to the CAS and the product identifies itself as a service point to Plex Manager in the CAS.

- TS user
  Users requesting views and attempting to perform actions in a MAINVIEW window require ESM authorization to protected resources. This occurs after the CAS initializes, a product identifies itself to the CAS, and the product initializes (whether it is in a separate PAS or not).

MAINVIEW Resources

The data displayed in views and the actions executed from views are considered MAINVIEW resources. Some resources are common to all MAINVIEW products. Common resources are managed by Plex Manager, which runs in the CAS. Other resources are specific to a MAINVIEW product, which runs in the PAS.

To control access to MAINVIEW resources, the resources must be identified to the ESM. There are hundreds of MAINVIEW resources, however, all of them can be identified by 13 resource definitions. The process of identifying these resources to the ESM is simplified by

- exploiting the naming convention used for resources
- using generic (or masking) characters when creating profiles, permits, or rules to control access to resources

The resource naming convention is described in the following section. Examples of combining the naming convention with the generic capabilites of your ESM are provided on page 113.

Resource Naming Convention

MAINVIEW resources are identified to an ESM by a resource class name and entity name.

Class Name: For MAINVIEW enhanced security, the default class for resources is $BBM, however, by default, it is translated automatically to FACILITY, which is a predefined to CA-ACF2, CA-Top Secret, and RACF. For information about using a class other than FACILITY, see Chapter 11, “Class Definitions” .

Entity Names: MAINVIEW resource entity names consist of multiple qualifiers separated by periods, similar to MVS data set names. Generally, the format of the entity name for data is

`BBM.`*product.context.inttable.suffix*

The format of the entity name for an action is

`BBM.`*product.context.intaction.suffix*

However, not all entity names follow this convention. Some entity names have additional qualifiers and some have fewer qualifiers. The entity name qualifiers are listed here.

BBM — The prefix for all MAINVIEW resources.

product — The ID of the product or service point in control of the window where data is being accessed or an action is being attempted. The ID can be as follows:

ID:	Product or Service Point:
CMF	CMF MONITOR
COMMON	Resources common to many products
MVALARM	MAINVIEW Alarm Manager
MVCICS	MAINVIEW for CICS
MVCSMON	Common Storage Monitor
MVDAC	MAINVIEW for DATA ACCELERATOR Compression
MVDB2	MAINVIEW for DB2
MVIMS	MAINVIEW for IMS
MVIP	MAINVIEW for IP
MVMQS	MAINVIEW for MQSeries (formerly known as Command MQ for S/390)
MVMVS	MAINVIEW for OS/390
MVSPS	MAINVIEW SYSPROG Services
MVUSS	MAINVIEW for UNIX System Services
MVVP	MAINVIEW VistaPoint
MVVTAM	MAINVIEW for VTAM
MVWEB	MAINVIEW for WebSphere
PLEXMGR	Plex Manager

context The context set in the window where the resource is being accessed. This qualifer is site-dependent.

inttable The internal ID of the table being accessed. The data displayed in a view is obtained from a table of information on a particular subject, such as CICS programs or DB2 subpools. Any number of views can display information from the same table. Some views obtain information from more than one table.

intaction The internal ID of an action being requested. This ID is usually the action name or an abbreviation of the action name.

suffix Indicates the type of resource and can be one of the following values:

Suffix:	Controls access to:
AA	any action.
AO	any action performed on the table currently accessed (*inttable*).
OA	any action performed on a row of data in a tabular view or the data displayed in a detail view.
OD	table data and, therefore, any view that displays data from that table.
CN	connection to a CAS and, therefore, access to the MAINVIEW environment.
TA	target context; without access, a user cannot select any product from the MAINVIEW selection menu.
TC	creation of a target context; without access, a PAS can not define itself as a PAS.
TH	global thresholds.

TS	trusted status of a PAS for inheriting a security environment.
PA	any product-level action, regardless of which view or table is accessed.
DATASET	data set name

#field The internal ID of a specific row of data for which an action has been specified.

ssid The subsystem identifier specified with the SSID parameter in the CAS and PAS started task procedures.

system The system identifier or system name where the target and MAINVIEW product are executing and from where resource access is occurring.

Finding Entity Names

Every MAINVIEW resource is defined in a resource definition, which includes the entity name of the resource. To determine the resource definition used for a particular view, see "Resource Definitions Listed by View" on page 265.

For a complete list of resource definitions and their corresponding entity names for each MAINVIEW product, see "Resources Definitions Listed by Product" on page 175.

In addition to those lists, the SERDEF view displays a single resource definition, including the entity name in the **Entity** field. For information on the SERDEF view, see "Browsing a Resource Definition" on page 168.

For more information about resource definitions, see "Using Security Views to Change Resource Attributes" on page 117.

Exploiting the Resource Naming Convention

The resource naming convention is designed to simplify the process of identifying resources to your ESM. When creating permits, profiles, or rules to control access to resources, an explicit or generic value can be specified for any qualifier in the entity name by using the masking characters supported by the ESM. The resource naming convention, combined with the generic capabilities of your ESM, allows you to identify hundreds of resources with just a few rules, profiles, or permits.

For example, to grant or deny access to any MAINVIEW function, you can define a single rule, profile, or permit that identifies a generic connect-to-CAS resource because, by default, all connect-to-CAS resources begin with BBM and end with CN:

In a CA-ACF2 rule:

```
$KEY(BBM.-.CN)
```

In a CA-Top Secret permit:

```
(BBM.*.CN)
```

In a RACF profile:

```
BBM.**.CN
```

Granting access to this resource would potentially allow access to any MAINVIEW function.

If you want to permit access to most tables (and therefore the views that display data from those tables), but deny access to certain tables, you might define a rule, permit, or profile that protects all of the table data resources, whose names, by default, begin with BBM and end with OD.

In a CA-ACF2 rule:

```
$KEY(BBM.-.-.-.OD)
```

In a CA-Top Secret permit:

```
(BBM.*.*.*.OD)
```

In a RACF profile:

```
BBM.**.OD
```

Then, you could define a rule, permit, or profile for a specific table:

In a CA-ACF2 rule:

```
$KEY(BBM.-.-.MYAG0.OD)
```

In a CA-Top Secret permit:

```
(BBM.*.*.MYAGO.OD)
```

In a RACF profile:

```
BBM.**.MYAGO.OD
```

For more information on creating rules, permits, and profiles, see Chapter 10, “Configuring Your ESM for Enhanced Security”.

Security Parameter Library

The default security parameter, class and resource definitions are distributed as members in the BBACTDEF library (do not modify these members). When you customize parameter, class and resource definitions using the security views, the customized definitions are saved in the security parameter library. This library is referenced by the BBSECURE DD statement in the CAS and PAS started task procedures. Its members are read during CAS and PAS initialization to establish security.

The security parameter library is created for you during AutoCustomization. If you did not use AutoCustomization and want to customize security definitions, you must create the security parameter library and define it in the CAS and PAS started task procedures as described in the *MAINVIEW Implementation Guide*.

The security parameter library contains the following members:

BBMTRN*nn*	Resource definitions for Plex Manager
BBMTSP*nn*	Class definitions for each known resource class
BBMTSS*nn*	Parameters definitions that specify the ESM and its attributes
BBMZRN*nn*	Common resource definitions used by all MAINVIEW products

Depending on which MAINVIEW products are installed, the security parameter library might also contain one or more of the following members:

ASTTRN*nn*	Resource definitions for MAINVIEW SYSPROG Services
BBDTRN*nn*	Resource definitions for CMF MONITOR and MAINVIEW for OS/390
BBFTRN*nn*	Resource definitions for MAINVIEW for IMS
BBHTRN*nn*	Resource definitions for MAINVIEW Alarm Manager
BBJTRN*nn*	Resource definitions for MAINVIEW VistaPoint
BBKTRN*nn*	Resource definitions for MAINVIEW for CICS
BBPTRN*nn*	Resource definitions for MAINVIEW for DB2
BBSTRN*nn*	Resource definitions for MAINVIEW for MQSeries (formerly known as Command MQ for S/390
BBUTRN*nn*	Resource definitions for MAINVIEW for UNIX Systems Services
BBWTRN*nn*	Resource definitions for MAINVIEW Explorer
DACTRN*nn*	Resource definitions for MAINVIEW for DATA ACCELERATOR Compression
TACTRN*nn*	Resource definitions for MAINVIEW for IP
SOPTRN*nn*	Resource definitions for MAINVIEW for VTAM
MVWTRN*nn*	Resource definitions for MAINVIEW for WebSphere

where *nn* is the two-character member name suffix. The default suffix is 00. The suffix enables you to create different versions of each member. The suffix for the parameter, class, and common resource definitions is associated to a CAS in the CASDEF view. The member suffix for product resource definitions is associated to a PAS in the TGTDEFD view.

Sharing a Security Parameter Library Between CASs

If you have a shared DASD environment, CASs that have the same security requirements can share a security parameter library by referencing the same library on the BBSECURE DD statement in each CAS started task procedure. This option eliminates the need to create or maintain separate security parameter libraries for each CAS.

If your CASs have different security requirements, you can still share the security parameter library, however, you must create the appropriate members with different member name suffixes and then use the CASDEF view to associate each CAS to the appropriate member suffix.

Views for Administering Enhanced Security

The generalized views for enhanced security are as follows:

EZSEC	Is an Easy Menu with hyperlinks to other security views.
SECURITY	Lists the security views. You can select a view from the list or place your cursor on the view and press Enter to hyperlink to the view.

The views for managing class definitions are as follows:

SECDEFL	Lists all the security parameter library resource class definition members. You can select a member for display or delete a member.
SECDEF	Displays a single class definition. Use this view to create, update, or delete a class definition.

For information about these views, see Chapter 11, “Class Definitions”.

The views for managing parameter definitions are as follows:

SEPDEFL	Lists the security parameter definition members. You can select a member for display or delete a member.
SEPDEF	Displays the contents of a member. You can use this view to change security parameters for the selected member or to create a new member.

For information about these views, see Chapter 12, “Parameter Definitions”.

The views for managing resource definitions are as follows:

EZSECRES	Is an extension of EZSEC that allows you to change the context or product before displaying product resources.
SERDEFP	Lists the active products for the current context when hyperlinking from EZSECRES.
SERDEFC	Lists the active targets for the product selected by hyperlinking from SERDEFP when hyperlinking from EZSECRES.
SERDEFOV	Lists the default and individual resource definitions for the current product and context.
SERDEFEX	Lists the individual resource definitions referenced by the default resource definition selected by hyperlinking from the +++ value in the `Exp` column in SERDEFOV.
SERDEFL	Lists all of the resource definition members. You can select a member for display or delete a member.
SERDEF	Displays a single resource definition. Use this view to create, change, enable, or disable a resource definition.

For information about these views, see Chapter 13, “Resource Definitions”.

Using Security Views to Change Resource Attributes

Each MAINVIEW resource has a corresponding resource definition. The resource definition contains the class and entity name for the resource, as well as other security attributes. Resources that have similar functions are grouped together and represented by a *default* resource definition. Changing the default resource definition provides a short-cut for changing multiple resource definitions. The individual resource definitions provide additional flexibility, allowing you to override the default resource definition.

To change resource definitions for a specific product, do the following:

1. From within PLEXMGR, type **EZSEC** on the COMMAND line. The EZSEC view is displayed, as shown in Figure 8.

```
04JAN2000  13:37:23 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                 SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
 W1 =EZSEC=============CXTSTJ===*========04JAN2000==13:37:22====PLEXMGR=======1
                                Security Menu

  Security Tasks
                            +----------------------+
. Review Class Definitions  |   Place cursor on    |
. Review Security Parms     |    menu item and     |
. Common Resources          |     press ENTER      |
> Product Resources         +----------------------+
```

Figure 8. EZSEC View

2. Hyperlink from the **Product Resources** field to display the EZSECRES view.
3. Hyperlink from the **Choose Another Product** field.

   A help panel is displayed that provides information on selecting a product. When you press the END key, the SERDEFP view is displayed.
4. Position the cursor on `MVMVS` in the **Product** column and press ENTER.

   A help panel is displayed that provides information on selecting a context. When you press the END key, the SERDEFC view is displayed with information on the contexts defined for MAINVIEW for OS/390.
5. Position the cursor on a context name in the **Context** column and press ENTER.

   A help panel is displayed that provides information on resource categories. When you press the END key, the SERDEFOV view is displayed, as shown in Figure 9.

```
21FEB2000  10:27:21 ----------- INFORMATION DISPLAY --------------------------
COMMAND  ===>                                                 SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
>W1 =SERDEFOV==========DXTSTI===*========(00 EDIT          )====MVMVS=========
CMD Description                             Enab Exp Change Comment
--- ------------                            ---- --- --------------
    Default - Table Data                    Yes  +++
    Default - Any Table Actions             Yes  +++
    Default - Primary Actions (All Views)   Yes  +++
    Default - Specific Table Action         Yes  +++
```

Figure 9. SERDEFOV View and Default Resource Definitions

Most MAINVIEW products have four default resource definitions. The default resource definitions for MAINVIEW for OS/390 are shown in Figure 9. The description for a default resource definition begins with the word `Default`, for example, `Default - Table Data`.

Changing a default resource definition changes all of the resource definitions represented by the default definition. For example, if you disable the `Default - Table Data` resource definition, you disable every resource definition represented by that default definition.

To display the individual resource definitions represented by the default definition, position the cursor on the +++ displayed in the **Exp** field of the SERDEFOV view and press ENTER. The SERDEFEX view, containing the individual resource definitions, is displayed, as shown in Figure 10.

```
21FEB2000  10:43:47 ----------- INFORMATION DISPLAY -------------------------
COMMAND  ===>                                                 SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
>W1 =SERDEFOV=SERDEFEX=DXTSTI===*========(00 BROWSE        )====MVMVS========
CMD Description                               Enab Change Comment
--- ------------                              ---- --------------
    Addr Space - Table Data                   Yes
    Addr Space across interval - Table Data   Yes
    Addr Space Device Use/Delay- Table Data   Yes
    Address Space Enq Use/Delay - Table Dat   Yes
    Address Space HSM Use/Delay - Table Dat   Yes
    Address Space JES Use/Delay - Table Dat   Yes
    Address Space MSG Use/Delay - Table Dat   Yes
    Addr Space in Workload - Table Data       Yes
    Address Space XCF Use/Delay - Table Dat   Yes
    Channel Path - Table Data                 Yes
    Channel Path on LCU - Table Data          Yes
    Common Storage - Table Data               Yes
```

Figure 10. SERDEFEX View and Individual Resource Definitions

For more information on changing resource definitions, see Chapter 13, “Resource Definitions”.

Establishing Enhanced Security

Establishing enhanced security involves the following steps:

1. Required. Make sure the user ID of the individual that will perform the following steps is authorized to access each CAS, and the security parameter library for each CAS, on each MVS image.

2. Optional. Change the class definition. If you want to use a resource class other than FACILITY, use the SECDEF view, as described in "Changing a Class" on page 149.

3. Optional. Change the parameter definition. The security parameter definition specifies which ESM is to be used. However, the distributed parameter definition automatically determines which ESM is active on the MVS image. Do not modify the parameter definition unless you

   – have both CA-ACF2 and RACF installed and want to use RACF

   – use the RACF GROUP feature, and do not want it inherited on a connected system

   – use an ESM other than RACF, CA-ACF2, or CA-Top Secret

   To change the parameter definition for any of these reasons, use the SEPDEF view, as described in "CHANGE SECURITY PARAMETERS Dialog" on page 158.

4. Required. Review the resource names for the common resources and product resources you want to protect.

   For an explanation of resource names, see "Resource Naming Convention" on page 111. To determine the resource definition used for a particular view, see "Resource Definitions Listed by View" on page 265. For a complete list of resource definitions and their corresponding entity names for each MAINVIEW product, see "Resources Definitions Listed by Product" on page 175.

5. Optional. Change the resource definitions. If any MAINVIEW resources are already identified to the ESM using a site-specific naming convention, you might want to change the MAINVIEW entity names to match that naming convention. For information on changing the entity name, class name, access intent, or logging attributes of a resource definition, see "Changing a Resource Definition" on page 169.

6. Required. Authorize the CAS and PAS started tasks, create rules, profiles, or permits to identify the resources to the ESM , and grant or deny access to the resources, as described in "Configuring Your ESM for Enhanced Security" on page 123.

7. Optional. If you created any new class, parameter, or common resource definitions members with a member name suffix other than 00, specify the new suffixes in the CASDEF view and reinitialize the CAS. If you created any new product resource definitions with a member name suffix other than 00, specify their suffix in the TGTDEFD view and reinitialize the PASs that use them. These members are listed and described in "Establishing Enhanced Security" on page 119.

Note: Some MAINVIEW products use both enhanced and basic security, as described in "Types of Security" on page 7. If any of your products use basic security, you must also follow the instructions in Part 2, "Basic Security".

Disabling Enhanced Security for All MAINVIEW Resources

You can disable all security if you decide you do not need MAINVIEW resources secured at this time. Use the following procedure to disable all enhanced security:

1. Display the MAINVIEW Selection Menu.
2. Select Option 1 for Plex Manager.
3. In the COMMAND line, enter **SEPDEF**.
4. In the COMMAND line, enter **EDIT** to request an edit session.
5. In the COMMAND line, enter **CHAnge**.
6. At the top of the Change Security Parameters dialog, specify **NONE** for **ESM Type**.
7. Press the END key and enter **SAVE** in the COMMAND line to save your change.
8. Reinitialize the CAS. Reinitializing the CAS disrupts any connected product address spaces and cross-system sessions on the local system (the CAS and all associated PASs).

Important

An ESM Type of NONE bypasses security for the entire subsystem (the CAS and all associated PASs). During CAS initialization, MAINVIEW requests ESM authorization using the following parameters:

Class name	FACILITY
Entity name	BBMSS.ESMTYPE.NONE

You must have a RACF profile, CA-Top Secret permit, or CA-ACF2 rule defined to authorize this request or CAS initialization terminates. See Chapter 10, “Configuring Your ESM for Enhanced Security” on page 123 for additional information.

If you do not have access to the SEPDEF view, use the following procedure to change the ESM type parameter:

1. Check the security parameter library for an existing BBMTSS00 member.

   If there is a BBMTSS00 member already, rename it if you want to keep these global security parameters.
2. Create a new member named BBMTSS00.
3. Add the following statement to the new member:

   ```
   ESM ESMTYPE(NONE);
   ```
4. Save the member.
5. Reinitialize the CAS. Reinitializing the CAS disrupts any connected product address spaces and cross-system sessions on the local system (the CAS and all associated PASs).

Determining Which Security Members Are Active

During CAS and PAS initialization, the parameter, class, and resource definition members in the security parameter library are read to establish the MAINVIEW security environment. There can be multiple versions of a member, each having a unique suffix. The default suffix is 00. This section explains how to determine which members are active for a CAS and PAS. For more information on the security parameter library, see page 119.

CAS Security Members

To display the security parameter members currently defined to the CAS:

1. Display the MAINVIEW Selection Menu.
2. Select Option 1 for Plex Manager.
3. Display the CASDEF view by entering **CASDEF** in the COMMAND line of Plex Manager.
4. Position the cursor on the name of the CAS in the **CAS Name** field and press ENTER to display the CASDEFD view.
5. Review the information in the **Parmlib Suffixes** section of this view.

   The suffixes for the security parameter library members defined to the CAS are shown in the following fields:

   SepDef Suffix Two-character suffix for the parameter definition member.

   SecDef Suffix Two-character suffix for the class definition member.

   Common Suffix Two-character suffix for the common resource definition member.
6. To see the current parameter definition member for the CAS:
   a. Display the SEPDEFL view by entering **SEPDEFL** in the COMMAND line of the Plex Manager product.
   b. Select the member with the same **Member Suffix** field value as the value shown in the CASDEFD **SepDef Suffix**. The SEPDEF view is displayed. For more information about this view, select its name from the window information line and press your HELP key.
7. To see the current class definition member used for all resource access authorizations made for both common and product-specific resources:
   a. Display the SECDEFL view by entering **SECDEFL** in the COMMAND line of the Plex Manager product.
   b. Select the member with the same **Member Suffix** field value as the value shown in the CASDEFD **SecDef Suffix** field. The SECDEF view is displayed. For more information about this view, select its name from the window information line and press your HELP key.
8. To see the current resource definition member used for common resource access authorizations:
   a. Display the SERDEFL view by entering **SERDEFL** in the COMMAND line of the Plex Manager product.

b. Select the member that has a **Product** description of `COMMON` and a **Member Suffix** value that is the same as the value shown in the **Common Suffix** field of the CASDEFD view.

For more information about these views, select the view name in the window information line with your cursor and press your HELP key.

PAS Security Member

To display the current resource definition member used for a specific MAINVIEW product:

1. Display the CASDEF view by entering **`CASDEF`** in the COMMAND line of the Plex Manager product.
2. Position the cursor on the name of the CAS in the **CAS Name** field and press ENTER to display the CASDEFD view.
3. Review the information in the **TgtDef Suffix** field of the **Parmlib Suffixes** section of this view. The **TgtDef Suffix** field value shows the two-character suffix for the target definition member in the security parameter library defined to the CAS. A target definition parameter member (see the TGTDEF view described in the *MAINVIEW Administration Guide*) specifies a
   - target for a specific product, such as PLXMGR on SYSA
   - resource definition member in the security parameter library for that product
4. Display the TGTDEFL view by entering **`TGTDEFL`** in the COMMAND line of Plex Manager.
5. Select the member with the same **Member Suffix** field value as the value shown in the CASDEFD **TgtDef Suffix** field. The TGTDEF view is displayed.
6. Look in the **Product** column of the TGTDEF view for the product you want, and then place the cursor on the name of the CAS in the **CAS Name** field in this view and press ENTER. The TGTDEFD view is displayed.
7. Check the suffix value from the **SerDef Suffix** field in the **Security Info** section of the TGTDEFD view.
8. To see the resource definition member in the security parameter library used for that product:
   a. Display the SERDEFL view by entering **`SERDEFL`** in the COMMAND line of a view from that product.
   b. Select the member with the same **Member Suffix** field value as the value shown in the **SerDef Suffix** field of the TGTDEFD view.

For Plex Manager, select the member with a **Product** field value of `PLEXMGR`, not `COMMON`.

For more information about these views, select the view name in the window information line with your cursor and press your HELP key.

Chapter 10. Configuring Your ESM for Enhanced Security

This chapter provides the instructions for customizing the CA-ACF2, RACF, and CA-TOP SECRET ESMs.

Configuring CA-ACF2

This section provides information about the administrative actions for CA-ACF2 that must be performed to support the MAINVIEW security interface.

Note: See Chapter 9, "Introduction to Enhanced Security" on page 109, for general information about the enhanced security functions.

To define the security subsystem to CA-ACF2:

1. Set the required CA-ACF2 Generalized System Options (GSO) record options; see "Step 1: Setting the Required GSO Record Options" on page 124, for instructions.
2. Define LOGONID(s) for the CAS and each PAS; see "Step 2: Authorizing the PAS and CAS" on page 124, for instructions.
3. Update the SAFDEF records; see "Step 3: Updating the CA-ACF2 SAFDEF List" on page 126 for instructions.
4. Optionally add SAF Resource Classes to CA-ACF2; see "Step 4: (Optional) Adding a SAF Resource Class to CA-ACF2" on page 127, for instructions.
5. Optionally define CA-ACF2 rules for controlling access to MAINVIEW resources; see "Step 5: (Optional) Defining Rules for Controlling View Resources" on page 129, for instructions.

Step 1: Setting the Required GSO Record Options

All required CA-ACF2 Generalized System Options (GSO) record options must be set correctly to support a full-function SAF-based security interface. A number of CA-ACF2 GSO records must have certain options specified.

To set the GSO record options:

1. Review the information in Table 12, which describes each required option setting, to determine the required options for your site.

Table 12. Settings for CA-ACF2 Global System Options

GSO record name	Required option	Description
PSWD	PSWDXTR	Enables RACROUTE EXTRACT to be executed. This option enables LOGONIDs with the BDT attribute to inherit a user's security environment from another address space or from another MVS image (remote system). **Note:** This option is not absolutely required. However, if it is not in effect, an ACF2 error message is issued for every address space that uses BMC Software product facilities, and there may be certain environments in which it is not possible to inherit LOGONIDs from another MVS image.
OPTS	STC	Enables started tasks to have security control block structures built to support SAF-based MUSASSs.

2. The following TSO commands illustrate how to set all the required options:

```
ACF
SET CONTROL(GSO)
CHANGE OPTS STC
CHANGE PSWD PSWDXTR
END
```

3. After the required options have been changed, use the following operator commands to cause them to take effect:

```
F ACF2,REFRESH(OPTS)
F ACF2,REFRESH(PSWD)
```

Step 2: Authorizing the PAS and CAS

LOGONIDs **must** be defined for the CAS and each PAS.

This step describes how to

- define LOGONIDs with the proper attributes
- associate the started task procedure names for the CAS and each PAS with the defined LOGONIDs

A CA-ACF2 LOGONID **must** be associated with each started task. The LOGONID must be able to execute as a started task and must be authorized to access all data sets used within the address space.

Note: The CAS **must** execute as a started task. PASs normally execute as started tasks, but this is not required. Most PASs can also execute as batch jobs.

A LOGONID for each address space is associated with that address space by the CA-ACF2 started task control (STCXIT) installation exit or by an exact name match between the started task name and an ACF2 LOGONID. The names of the associated LOGONIDs need not match the names of the started procedures. However, if they do **not** match, you must use CA-ACF2's STCXIT to establish the correspondence between each started task procedure name and its associated LOGONID.

If you do not explicitly assign a LOGONID in your CA-ACF2 started task control exit, STCXIT, and if the name of the started task procedure does not have a corresponding matching LOGONID, the LOGONID specified in the GSO OPTS record DFTSTC parameter is assigned by CA-ACF2. Typically, this LOGONID **cannot** be used successfully, because specific attributes are required for the LOGONID (such as MUSASS) that is used with the address spaces; these attributes typically are not specified for the default STC LOGONID.

For additional information about the CA-ACF2 started task control exit, see the *CA-ACF2 System Programmer's Guide*.

To define LOGONIDs for the started tasks:

1. Use the following TSO commands, which illustrate how to define LOGONIDs for the CAS and a PAS:

```
ACF
SET LID
INSERT USING(ACFSTCID) BBMCAS   NAME(CAS)                    +
                                STC SOURCE(STCINRDR) NOTSO   +
                                MUSASS JOBFROM NO-SMC BDT    +
                                RESTRICT
INSERT USING(ACFSTCID) BBMPAS   NAME(PAS)                    +
                                STC SOURCE(STCINRDR) NOTSO   +
                                MUSASS JOBFROM NO-SMC BDT    +
                                RESTRICT
END
```

Notes:

- The `MUSASS` attribute on the LOGONIDs is **required**.
- The `JOBFROM` and `NO-SMC` attributes are required, but will be set automatically at execution time if not previously established as attributes for each LOGONID.
- The `BDT` attribute on the LOGONIDs is **required**. This attribute enables the PSWDXTR GSO PSWD record option to be effective, permitting the CAS and PAS to inherit security environments from user address spaces.

2. Associate the CAS and PAS LOGONIDs with their started task procedure names.

   The LOGONID used for a started task address space is determined by the CA-ACF2 Started Task Validation Exit (STCXIT). The name of the started task validation exit is specified by the STCXIT parameter of the EXIT GSO record. If your enterprise has coded an STCXIT, you must associate the LOGONID(s) with the started task procedure names defined for the PAS(s) and CAS.

   If your enterprise does not have an active STCXIT that can perform this function, the LOGONID used by CA-ACF2 defaults to the started procedure name, if a LOGONID with a matching name is defined. Otherwise, the default started task LOGONID (ACFSTCID) is used, which typically **cannot** be used successfully, because it is not likely to have both the `MUSASS` and `BDT` attributes.

Step 3: Updating the CA-ACF2 SAFDEF List

For the CA-ACF2 6.*n* SAF interface to process the calls to CA-ACF2, the CA-ACF2 SAFDEF records must be updated with specifications concerning the control points where the RACROUTE calls are being made. CA-ACF2 6.*n* does not process RACROUTE calls unless you have explicitly instructed it to do so by updating the SAFDEF records.

The MAINVIEW security interface passes control point identification information to CA-ACF2 using the `SUBSYS=` and `REQSTOR=` parameters of the RACROUTE macro instruction. To customize these values, use the SEPDEF view, as discussed in Chapter 12, “Parameter Definitions” on page 155, and the SERDEF view, as discussed in Chapter 13, “Resource Definitions” on page 163.

1. Use the SEPDEF view in Plex Manager to customize these parameters by changing the field values for SUBSYS and REQSTOR in the appropriate Global Security Parameters member of the security parameter library (DDname BBSECURE).

   The default for these parameters is as follows:

   SUBSYS The MVS Subsystem ID (SSID) defined for use by the CAS.

   REQSTOR Not altered by the security interface. Defaults to the value specified for each resource in the resource definition table (either `COMMON` or client product-specific), which typically is the name of the module or subroutine where the resource manager initiated the call to CA-ACF2.

2. Once you have customized BBMTSS*nn* (and possibly altered the `SUBSYS(`*`SSID`*`)` parameter from its default value) using the SEPDEF view, enable CA-ACF2 to process security invocations by specifying the selected SUBSYS value in a CA-ACF2 SAFDEF record. Here is a sample TSO command for this specification:

   ```
   ACF
   SET CONTROL(GSO)
   INSERT SAFDEF.BBCS ID(BBCS) MODE(GLOBAL)REP
   RACROUTE(SUBSYS=BBCS   REQSTOR=-)
   END
   ```

   In this example, the MVS SSID selected for use with the CAS is `BBCS`.

3. After the new SAFDEF record is inserted, the in-storage SAFDEF list must be refreshed. To do this, issue the operator command:

   ```
   F ACF2,REFRESH(SAFDEF)
   ```

Step 4: (Optional) Adding a SAF Resource Class to CA-ACF2

Note: Skip this step if you plan to use the class name FACILITY.

Before you define unique generalized resource rules, you may need to define one or more new SAF resource classes to CA-ACF2.

Access to the CAS and PAS resources are, by default, protected by generalized resource rules in external SAF class `FACILITY` (internal class `$BBM`, which is, by default, transformed to external class `FACILITY`).

If you want to use external SAF resource class `FACILITY`, you should have already mapped SAF resource class `FACILITY` to some CA-ACF2 generalized resource rule type. This is usually rule type `FAC`, the CA-ACF2 default.

If you do not want to use external SAF resource class `FACILITY`, you need to use the SECDEF view to customize the resource class definition table, member BBMTSP*nn*, which resides in the CAS security parameter library (DDname BBSECURE), and alter resource class `$BBM` to change the external SAF resource class that internal class `$BBM` translates to (the `NEXT` parameter). You may use any SAF resource class that you want, including `DATASET`.

Note: Certain resources that use SAF class `FACILITY` cannot be customized. In the following discussions of these resources, this fact is noted when appropriate.

To support other external SAF resource classes in an MVS system with CA-ACF2, you must define the rule type to which ACF2 is to map the external SAF resource class. To do this, you must add new CLASMAP records. The CLASMAP GSO records specify the correspondence between a SAF resource *class* name and its associated CA-ACF2 generalized resource rule *type*.

1. Select the CA-ACF2 resource rule types that you will use to define the rules to control access to product resources.
2. Update the CA-ACF2 CLASMAP records. The following lines are example TSO commands you could use:

   ```
   ACF
   SET CONTROL(GSO)
   INSERT CLASMAP.class       +
          RESOURCE(class)     +
          RSRCTYPE(type)      +
          ENTITYLN(39)
   END
   ```

3. Refresh the in-storage copy of the CLASMAP tables using the following operator command:

   ```
   F ACF2,REFRESH(CLASMAP)
   ```

4. If you want to make the rules for the selected resource types resident (this is not required), use TSO commands like the following examples:

   a. To add rule types to the INFODIR GSO record:

      ```
      ACF
      SET CONTROL(GSO)
      ```

```
CHANGE INFODIR ADD TYPES(R-Rtype)
END
```

Notes:

- If your CA-ACF2 configuration has not already been updated to use INFODIR GSO records instead of RESDIR, use the following command to add the rule type to the list for which in-storage directories will be constructed at CA-ACF2 initialization:

  ```
  CHANGE RESDIR ADD TYPES(R-type)
  ```

- Resident rule directories with transient rule data are not supported. For all rule types referred to by the security interface, if they are to be made resident by CA-ACF2, you must specify TYPES(R-R*type*).

b. To refresh the RESDIR information:

```
F ACF2,REFRESH(RESDIR)
```

c. To refresh the in-storage INFODIR data:

```
F ACF2,REFRESH(INFODIR)
```

d. To build (or rebuild) the in-storage directory for a rule type:

```
F ACF2,REBUILD(type)
```

Nonresident rules with masked rule keys for CAS and Plex Manager resources **are not supported**. So, if your product-referenced rules are not globally resident, you must direct CA-ACF2 to build a (globally) resident rule directory, as in Step 6, above, or you must direct the product to build a directory and to bring the rules into private storage (LSQA) when required.

A directory can be built and the resource rules brought into private storage by altering the `RESDIR` parameter in the ACF2 section of the external SAF resource classes involved. Use the SECDEF view to customize the resource class definition member BBMTSP*nn* in the CAS security parameter library.

Step 5: (Optional) Defining Rules for Controlling View Resources

To control view resources, you use generalized resource rules or ordinary data set rules, or both.

Before you apply the information in this section, review your CA-ACF2 configuration to ensure that the following requirements are met:

- The LOGONIDs for all users should be defined to CA-ACF2 in each MVS system. For any end user, the LOGONID must be the same in every MVS system.

  If your enterprise is required to use the GSO PSWD record PSWDXTR option, the password for each LOGONID must be the same on each MVS system. Normally, this will not be required (and so passwords for the same LOGONID on multiple systems do not need to be synchronized).

- End user access authority should be defined to CA-ACF2 in a consistent manner in all MVS systems.

You can create resource rules or you can use ordinary data set rules to protect resources. You must consider the following points and determine which approach best suits the needs of your enterprise:

- You can use either ordinary data set rules or generalized resource rules to specify how CA-ACF2 is to control access to resources.
- Ordinary data set rules are used by translating the resource entity names to *pseudo data set* names and the resource class name to `DATASET`.

Each choice has advantages and disadvantages, which differ from one enterprise to another, depending upon the following conditions:

- How familiar your security administration personnel are with generalized resource rules and the facilities and procedures in place to manipulate them
- The extent to which the RACF style of generic resource entity name construction is to be used
- Whether or not CA-ACF2 Release 6.1 or 6.2 is in use

The resource entity names shown as examples translate most directly to ordinary CA-ACF2 data set rules. However, your enterprise may have standards that prohibit the use of data set rules for any resource that is not, in fact, a data set. You may, therefore, be required to use CA-ACF2 generalized resource rules. See the following sections for more information:

- "Using Ordinary CA-ACF2 Data Set Rules with SAF Resource Classes" on page 130
- "Using Generalized CA-ACF2 Resource Rules with SAF Resource Classes" on page 130

Using Ordinary CA-ACF2 Data Set Rules with SAF Resource Classes

If you choose to use ordinary CA-ACF2 data set rules, review "Step 5: (Optional) Defining Rules for Controlling View Resources" on page 129.

Use the SECDEF view to customize the resource class definition table, member BBMTSP*nn* of the CAS security parameter library (DDname BBSECURE) to specify that the internal resource class, `$BBM`, is to be translated to an external class DATASET (the `NEXT` parameter).

You need to indicate that authorization requests for resources should be validated using rules for the resource class DATASET (that is, ordinary CA-ACF2 data set rules). To do this, customize the class definition entry for internal class `$BBM` to indicate that the `NEXT` class is `DATASET`.

Because the default resource entity names are not likely to adhere to your existing data set naming convention, you should transform the resource entity name. You can prefix the resource entity name with a constant character string to add, in effect, a specific high-level qualifier to the pseudo data set name, unless the default, `BBM.`, is acceptable.

For example, if `BBM.` conflicts with your existing data set naming convention, but `$BBM.` does not, you could specify in BBMTSP*nn* a PREFIX (an entity name prefix) string of `$` for internal resource class `$BBM`. Thus `$` will be prefixed to all the entity names, which, by default, begin with `BBM.`, resulting in pseudo data set names that begin with a high-level qualifier of `$BBM`. Use the SEPDEF view to specify a prefix for class `$BBM`, which will be applied before class name transformation (the `NEXT` parameter).

The following examples show how you can define ordinary data set rules to control view resources. The ordinary data set rule examples assume you have transformed class `$BBM` to `DATASET` and prefixed the entity name with a $ (US dollar sign).

- To prohibit the use of the views and related action commands associated with the DIAGMSG view universally, specify

```
$KEY($BBM)
$MODE(ABORT)
 -.-.MYA40.- UID(-)
```

- To permit READ access to users whose UID string begins with OPER, specify

```
$KEY($BBM)
$MODE(ABORT)
 -.-.MYA40.- UID(OPER) READ(A)
 -.-.MYA40.- UID(-)
```

Using Generalized CA-ACF2 Resource Rules with SAF Resource Classes

If your enterprise standards permit you to take advantage of the improvements made to the generalized resource rules starting with CA-ACF2 Release 6.0, many former restrictions may no longer apply. Thus, with CA-ACF2 6.1 and later, resource rules may be acceptable, from an ease-of-use perspective.

Note: CA-ACF2-imposed restrictions may still limit your ability to use resource rules. For example, RACROUTE FASTAUTH calls cannot be used with masked resource rule keys until Release 6.1, and NEXTKEY cannot be used in resource rules referenced through FASTAUTH until Release 6.2.

Alternatively, your enterprise may choose not to use CA-ACF2's rule key masking character choices to define the rules that control view resources. In this case, you do not need the additional function and features enabled by the use of ordinary CA-ACF2 data set rules. In either case, your use of all CA-ACF2 rule specification facilities is fully supported and is subject only to CA-ACF2 limitations.

The following examples show how you can define generalized resource rules to control access to resources:

- To prohibit the use of the views and view action commands associated with the DIAGMSG view in the MAINVIEW for OS/390 product in context SYSP#2, specify

  ```
  $KEY(BBM.MVMVS.SYSP#2.MYA40  UID(-) PREVENT
  ```

- To permit access by users whose UID string begins with OPER, specify

  ```
  $KEY(BBM.MVMVS.SYSP#2.MYA40  UID(OPER) SERVICE(READ) ALLOW
   UID(-) PREVENT
  ```

Configuring RACF

This section provides information about the administrative actions for RACF (Version 1.8 and later) that must be performed to support the MAINVIEW security interface.

Note: See Chapter 9, "Introduction to Enhanced Security" on page 109, for general information about the security functions. To define the security subsystem to RACF:

1. Define security attributes for started tasks; see "Step 1: Authorizing the CAS and PAS" on page 132.
2. Optionally, add resource classes to RACF for resources; see "Step 2: (Optional) Adding Resource Classes to RACF" on page 133.
3. Create security profiles for resources; see "Step 3: Creating RACF Security Profiles" on page 135.
4. Specify security profiles to control access to resources; see "Step 4: Specifying Profiles to Control Access to Product Resources" on page 136.

Step 1: Authorizing the CAS and PAS

The CAS and MVS PAS run as started tasks. Therefore, you must associate the procedure names for the CAS and PAS with a suitably authorized user ID, using the STARTED class or the started procedures table ICHRIN03.

When a started task is initiated, RACF checks to see if the STARTED class is active. If it is active, RACF looks for a matching profile in the STARTED class to determine the user ID and group ID for the started task. A generic profile such as ** or *.* with a valid STDATA segment will be selected in the absence of a more specific one and will therefore effectively override any entry in ICHRIN03. If there is no applicable profile in the STARTED class, RACF will use the started procedures table, ICHRIN03, to determine the user ID and group ID to be used for the started task. If the STARTED class is not active, RACF only uses the started procedures table, ICHRIN03.

Note: If the user ID and group ID assigned by the selected STARTED class profile or entry in the started procedures table, ICHRIN03, are not defined to RACF, the started tasks execute with only the limited authority of an undefined user. In this case, the address space is able to access protected resources only if the universal access authority for the resource is sufficient to allow the requested operation.

To define started task user IDs:

1. Define CAS and PAS user IDs.

   The following example RACF commands illustrate how to define user IDs for the CAS and PAS:

   ```
   ADDUSER BBMCAS DFLTGRP(SYSMGMT) OWNER(SYSPROG)
   ADDUSER BBMPAS DFLTGRP(SYSMGMT) OWNER(SYSPROG)
   ```

   Note that no special attributes, such as OPERATIONS, are required for the RACF user IDs associated with the CAS and PAS. In fact, it is highly desirable that user IDs **without** any special attributes be used for these address spaces.

2. Define the CAS and PAS started tasks.

The following example RACF commands illustrate how to associate the previously defined user IDs to a specific started procedure name. In this example, we assume that the procedure names that are being used are BBICAS and BBIPAS:

```
RDEFINE STARTED BBICAS.* OWNER(SYSPROG)       +
STDATA(USER(BBMCAS) GROUP(SYSMGMT))
RDEFINE STARTED BBIPAS.* OWNER(SYSPROG)       +
STDATA(USER(BBMPAS) GROUP(SYSMGMT))
SETROPTS RACLIST(STARTED) REFRESH
```

For additional information about defining profiles in the STARTED class or adding entries to the RACF started procedures table, ICHRIN03, see the *OS/390 Security Server (RACF) Security Administrator's Guide (IBM)* manual.

Step 2: (Optional) Adding Resource Classes to RACF

If you want resource access authorizations to use SAF class `FACILITY`, no further customization is necessary because `FACILITY` is already defined in the RACF CDT and RTB for all supported releases of RACF.

Security can be customized to use one or more resource classes other than the default, `FACILITY`. The following sections show you how to add an additional SAF resource class to ICHRRCDE, the RACF class descriptor table (CDT), and to ICHRFR01, the RACF router table (RTB), and how to specify profiles that control access to CAS and product resources.

The resource class names for most resources are entirely variable and are based on a naming convention that is shown in the SERDEF detail views, SERDEFD or SERDEFE, for a specific resource. The detail views are accessed through the SERDEF view; see Chapter 13, "Resource Definitions" on page 163, for more information. BMC Software ESM security provides default values, but you can change the default to specify an existing resource class that is already defined, and you can change the default entity names to specify existing profiles that are already defined.

When you are using RACF and you do not want to use SAF resource class `FACILITY`, you need to do the following:

1. Customize the resource class definition table, member BBMTSP*nn* of the CAS security parameter library (DDname BBSECURE).

   For detailed information, see Chapter 13, "Resource Definitions" on page 163.

   Note: Certain resource names that use SAF class `FACILITY` cannot be customized. In the following discussions of these resources, this fact is noted when appropriate.

2. Create or update ICHRRCDE, the RACF resource class descriptor table, as follows:

a. Code the ICHERCDE macro for each class.

Figure 11 is an example of the code for the ICHRRCDE table.

```
TITLE 'RACF RESOURCE CLASS DESCRIPTOR TABLE - ICHRRCDE'
  *
  *
  class ICHERCDE CLASS=class,
                 ID=id,                                    X
                 POSIT=posit,                              X
                 FIRST=ANY,                                X
                 OTHER=ANY,                                X
                 MAXLNTH=44,        or larger, if necessary X
                 RACLIST=ALLOWED,                          X
                 OPER=NO
  *
  *  NULL ENTRY MUST BE LAST ENTRY
  *
           END
```

Figure 11. Example of Source Code for the RACF ICHRRCDE Table

Note: The values shown in the example may not be applicable to your site requirements.

If an ICHRRCDE member already exists, add the new class entries to the existing source and proceed with the assembly and link edit steps.

b. Assemble the source.

When you assemble the ICHRRCDE table, the following MNOTES may be generated for a new class entry:

```
4,*** CLASS NAME DOES NOT CONTAIN NATIONAL CHARACTER   OR DIGIT IN    X
           FIRST FOUR POSITIONS ***
4,*** ID VALUE NOT WITHIN RECOMMENDED RANGE (128-255) ***
4,*** POSIT VALUE NOT WITHIN RECOMMENDED RANGE (19-56) ***
```

These are only warnings; they should be ignored.

c. Link edit the resulting object module, replacing the current ICHRRCDE load module.

3. To create or update ICHRFR01, the RACF router table:

a. Code the ICHRFRTB macro for each class.

Figure 12 is an example of the code for the ICHRFR01 table.

```
TITLE 'RACF ROUTER TABLE - ICHRFR01'
  *
  *
  class  ICHRFRTB CLASS=class,                          X
               ACTION=RACF
  *
           ICHRFRTB TYPE=END
  *
           END
```

Figure 12. Example of Source Code for the RACF ICHRFR01 Table

If an ICHRFR01 member already exists, add the class entries to the current source and proceed with the assembly and link edit steps.

b. Assemble the source.

When you assemble this table, the following MNOTE may be generated for a new class entry:

```
4,*** CLASS NAME DOES NOT CONTAIN NATIONAL CHARACTER    OR DIGIT IN    X
             FIRST FOUR POSITIONS ***
```

This is only a warning; it should be ignored.

c. Link edit the resulting object module, replacing the current ICHRFR01 load module.

4. To put the change into effect, IPL MVS.
5. Issue the following three commands for each new class, if appropriate:

```
SETROPTS CLASSACT(class)
SETROPTS GENERIC(class)   (if generic profiles will be used)
SETROPTS GENCMD(class)    (if generic profiles will be used)
```

For additional information about installing entries in the CDT and RTB, see the IBM *System Programming Library: RACF* manual.

Step 3: Creating RACF Security Profiles

Note: Before you define unique security profiles, you may need to define additional SAF resource classes to RACF. See "Step 2: (Optional) Adding Resource Classes to RACF" on page 133 for more information.

To protect resources, you can define security profiles to RACF and then customize the resource definition tables for each product to use those profiles.

User IDs that you intend to associate with these profiles have the following requirements:

- The user IDs for all users of windows-mode client products should be defined to RACF in each MVS system where these products are running. For each user, the ID must be the same for each MVS system.
- For each user, the password must be the same on all connected systems.

Note: If the release level of RACF on all connected systems is 1.9 or above, this requirement does not apply.

- User access authority to resources should be defined to RACF in a consistent manner in all MVS systems where MAINVIEW products are running.

Step 4: Specifying Profiles to Control Access to Product Resources

When you define RACF security profiles, you can use * (one asterisk) and ** (two consecutive asterisks) to represent one or more index levels in the profile (entity) name.

Most resource entity names are entirely variable and can be customized at any level. You can establish profiles that control access to systems, products, view tables, and view action commands associated with a specific product resource, as shown in the following examples.

Example 1: To prohibit the use of a resource universally, use the following RDEFINE command syntax:

```
RDEFINE FACILITY                    +
        BBM.resource.name           +
        UACC(NONE)                  +
        NOTIFY(user ID)
```

where

`FACILITY` Is the name of the SAF resource class being used for this resource.

`BBM.`*resource.name* Is the entity name of the resource; see the SERDEF detail views, SERDEFD or SERDEFE, for this value. These detail views are accessed through the SERDEF view by placing your cursor on the resource name and pressing ENTER.

`UACC(NONE)` Is the RACF universal access to resource.

`NOTIFY(`*user ID*`)` Is the user ID to notify if violations occur.

Example 2: To permit READ access to users in a particular group, specify the following command:

```
PERMIT  BBM.resource.name           +
        CLASS(FACILITY)             +
        ACCESS(READ)                +
        ID(group)
```

where

`BBM.`*resource.name* Is the entity name of the resource; see the SERDEF detail views, SERDEFD or SERDEFE, for this value. These detail views are accessed through the SERDEF view by placing your cursor on the resource name and pressing ENTER.

`CLASS(FACILITY)` Is the name of the SAF resource class being used for this resource.

`ACCESS(READ)` Is the RACF access level being permitted (READ).

`ID(`*group*`)` Is the group identity being granted READ access.

Example 3: To permit UPDATE access by a specific user, specify the following command:

```
PERMIT  BBM.resource.name          +
        CLASS(FACILITY)            +
        ACCESS(UPDATE)             +
        ID(user)
```

where

`BBM`.*resource.name*	Is the entity name of the SAF resource; see the SERDEF detail views, SERDEFD or SERDEFE, for this value. These detail views are accessed through the SERDEF view by placing your cursor on the resource name and pressing ENTER.
`CLASS(FACILITY)`	Is the name of the SAF resource class being used for this resource.
`ACCESS(UPDATE)`	Is the RACF access level being permitted (UPDATE).
`ID`(*user*)	Is the user ID being granted access.

Configuring CA-TOP SECRET

This section provides information about the administrative actions for CA-TOP SECRET that must be performed to support the MAINVIEW security interface. Security supports CA-TOP SECRET Release 4.2 and later.

Note: See Chapter 9, "Introduction to Enhanced Security" on page 109, for general information about the security functions. To define the security subsystem to CA-TOP SECRET:

1. Define a new CA-TOP SECRET Facility Matrix entry; see "Step 1: Defining a New CA-TOP SECRET Facility Matrix Entry" on page 139.
2. Define security attributes for started tasks; see "Step 2: Authorizing the CAS and PAS" on page 140.
3. Optionally, update the Resource Definition Table Record to define new resource classes; see "Step 3: (Optional) Adding a New SAF Resource Class" on page 141.
4. Define ownership of resources by prefix name; see "Step 4: Defining Ownership of Resources" on page 142.
5. Control access to resources permitting access to prefixed resources; see "Step 5: Controlling Access to Product Resources" on page 143.

Step 1: Defining a New CA-TOP SECRET Facility Matrix Entry

You must define a new entry (or redefine an existing entry) in your CA-TOP SECRET Facility Matrix to set the CA-TOP SECRET control options for MAINVIEW security interface processing.

To accomplish this requirement most easily, select one of the unused, predefined USER facilities provided by CA-TOP SECRET, change its name, and modify the security attributes according to the requirements in the list of statements below.

Include these statements in the TSSPARMS data set, in which the USER9 facility (for example) is configured:

Note: In the following list of statements, `USER9` and `BBI3` are examples only.

```
FACILITY(USER9=NAME=BBI3)     * Required
FACILITY(BBI3=PGM=BBM)        * Required
FACILITY(BBI3=MULTIUSER)      * Required
FACILITY(BBI3=NOABEND)        * Required
FACILITY(BBI3=ACTIVE)         * Required
FACILITY(BBI3=SIGN(M))        * Required
FACILITY(BBI3=TENV)           * Required
FACILITY(BBI3=NONPWR)         * Required
FACILITY(BBI3=NOTSOC)         * Required
FACILITY(BBI3=NOPROMPT)       * Required
FACILITY(BBI3=TYPE=CICS)      * Required
FACILITY(BBI3=NOMRO)          * Required
FACILITY(BBI3=FACMATRX=YES)   * Required
FACILITY(BBI3=EXTSEC=YES)     * Required
FACILITY(BBI3=XFCT=YES)       * Required
FACILITY(BBI3=DSNCHECK=YES)   * Required
FACILITY(BBI3=RES)            * Required
FACILITY(BBI3=MAXUSER=500)    * Default (3000) is excessive
FACILITY(BBI3=ASUBM)          * Recommended
FACILITY(BBI3=MODE=FAIL)      * Recommended
FACILITY(BBI3=WARNPW)         * Recommended
FACILITY(BBI3=DORMPW)         * Recommended
FACILITY(BBI3=SHRPRF)         * Recommended
FACILITY(BBI3=LUMSG)          * Recommended
FACILITY(BBI3=STMSG)          * Recommended
FACILITY(BBI3=LCFTRANS)       * Recommended
```

Note: In the above example, the following TSSPARMS statements required in Release 4.2 are obsolete in Release 4.3 and later:

```
FACILITY(BBI3=TENV)
FACILITY(BBI3=NOMRO)
```

Step 2: Authorizing the CAS and PAS

To define security attributes for the CAS and PAS started tasks, you must

1. Define ACIDs for the CAS and each PAS and associate them with the Facility Matrix entry established for use by BMC Software ESM products.
2. Associate the started task procedure names for the CAS (and each PAS, if run as a started task) with the appropriate ACIDs (either existing or newly defined).

If you run the CAS and MVS PAS as started tasks, you must associate the appropriate procedure names with a suitably authorized ACID, using the TSS ADDTO(STC) command. The ACID must be able to access the STC facility and must be authorized to access all data sets used within the address space. Each ACID is associated with an address space by the CA-TOP SECRET STC table.

Note: Appropriately authorized ACIDs **must** be assigned to the started task procedures that you use to run the CAS and any PAS, because the ACID's MASTFAC attribute must specify the name of a properly configured CA-TOP SECRET Facility Matrix entry.

If you do not assign a specific, properly configured ACID for the started task procedures, the default assigned by CA-TOP SECRET probably **will not** work correctly.

For additional information about connecting started task procedures to ACIDs and Facility Matrix entries, see the *CA-TOP SECRET TSS Command Functions Guide*.

To define started task ACIDs:

1. Define CAS and PAS ACIDs.

   The following example TSS command illustrates how to define an ACID for the CAS and associate the CAS with the proper Facility Matrix entry:

   ```
   TSS CREATE(BBMCAS) NAME('SYSA CAS') FACILITY(STC) +
   PASSWORD(NOPW,0) DEPT(deptacid) MASTFAC(BBI3)
   ```

   In this example, `BBMCAS` is the ACID that is being defined for use by the `SYSA CAS`. The name that was previously selected for the Facility Matrix entry to be used is `BBI3.` If PASs are run as started tasks, ACIDs must be established for them in the same way they are for the CAS. The same Facility Matrix entry may be used for a PAS as is used for the CAS. There is no need to define another one. For example:

   ```
   TSS CREATE(BBMPAS) NAME('SYSA PAS')   +
       FACILITY(STC) PASSWORD(NOPW,0)    +
       DEPT(deptacid) MASTFAC(BBI3)
   ```

2. Define the CAS and PAS as started tasks.

   Defining a started task to CA-TOP SECRET results in the association of that started task with a specified ACID. The following TSS command illustrates how to define the CAS procedure, with a name of BBICAS, to CA-TOP SECRET as a started task, which is to use the previously defined ACID of `BBMCAS`:

   ```
   TSS ADDTO(STC) PROC(BBICAS)   ACID(BBMCAS)
   ```

Note: If PASs are run as started tasks, they must be added to the STC table just as they are for the CAS. For example:

```
TSS ADDTO(STC) PROC(BBIPAS)   ACID(BBMPAS)
```

Step 3: (Optional) Adding a New SAF Resource Class

Skip this step if you plan to use the class name FACILITY.

To define new SAF resource classes to CA-TOP SECRET, you must update the CA-TOP SECRET resource definition table (RDT) record (reserved ACID).

Note: Because the MAINVIEW security interface can use any class name you specify, adding a new resource class may not be necessary. New SAF resource classes are required by your site only if you are unable or do not want to use class `FACILITY`, which is internally transformed by CA-TOP SECRET to `IBMFAC`.

The manner in which this is done is release-dependent. Here is an example for CA-TOP SECRET Release 4.3:

```
TSS ADDTO(RDT)  RESCLASS(class)            +
    RESCODE(3B) ATTR(PRIVPGM,LONG,GENERIC) +
    ACLST(NONE,READ,UPDATE,ALL)            +
    DEFACC(NONE)
```

where *class* is a new user-defined class name to be used by security. The choice of X'3B' for the two-digit hexadecimal `RESCODE` is an example only. You must choose a resource code within the range permitted by CA-TOP SECRET (X'01' through X'3F' for Release 4.3), and it must not conflict with any previous choice you have made for another enterprise-defined resource class that has been added to the RDT.

The attributes LONG and GENERIC are required.

Another attribute you should consider for this resource class is NODEFPROT, because it causes CA-TOP SECRET to behave more like RACF with respect to this resource class; it is not required, however.

Other attributes (such as EXIT) may be set according to existing installation requirements, procedures, and practices.

The access levels shown, NONE, READ, UPDATE, and ALL, are also only examples. You may choose your own access level names.

Note: The default hexadecimal values associated with the access levels READ and UPDATE are the only values supported; you must ensure that your alternative access level names include these values.

The default access level of NONE is only an example. You may choose any default access level.

To control access to product resources, you must `ADD` the prefix of `BBM` to the resource class (that is, define ownership) and permit access to resources, by prefix name, that are by default in SAF class `FACILITY`.

Note: CA-TOP SECRET refers to internal SAF class `FACILITY` as `IBMFAC` externally. The MAINVIEW security interface can be customized to use a class other than `FACILITY` (that is, `IBMFAC`).

When you are using CA-TOP SECRET and you want to use SAF resource class `FACILITY`, use the standard CA-TOP SECRET RDT entry (class) of `IBMFAC` for the appropriate ADDTOs and PERMITs; for example:

```
TSS ADDTO(ownacid) IBMFAC(BBM)
```

When you are using CA-TOP SECRET and you do not want the SAF resource class `FACILITY` to be used, you need to customize the resource class definition table, member BBMTSP*nn* of the CAS security parameter library (DDname BBSECURE). For more information, see Chapter 13, "Resource Definitions" on page 163.

Note: Certain resources that use SAF class `FACILITY` cannot be customized.

Step 4: Defining Ownership of Resources

As with all CA-TOP SECRET resources, you must first define ownership of the resource name prefixes to CA-TOP SECRET by using the TSS ADDTO command. The following TSS commands perform this function:

```
TSS ADDTO(ownacid) class(BBM)
```

where

class Is the SAF resource class name selected.

`BBM` Is the high-level prefix of the resource names to be owned in the specified resource class name.

You **must** define ownership of the product resources to protect resources (that is, issue the `TSS PERMIT` command).

ACIDs that you intend to associate with these resources have the following requirements:

- The ACIDs for all users of MAINVIEW security interface-based products should be defined to CA-TOP SECRET in each MVS system that is used by the interface (see "Step 2: Authorizing the CAS and PAS" on page 140 for more information). For each user, the ACID must be the same for each MVS system.
- Each user's password must be the same on all connected systems.

  The CA-TOP SECRET database master encryption key also must be the same on all connected systems.

  Note: These requirements do not apply to recent maintenance levels of CA-TOP SECRET Release 4.3 and later.
- User access authority to product resources should be defined to CA-TOP SECRET in a consistent manner in all MVS systems used by the MAINVIEW security interface.

Before defining ownership of resources, you may need to add additional SAF resource classes to the CA-TOP SECRET RDT (see "Step 3: (Optional) Adding a New SAF Resource Class"

on page 141 for more information). Once the resources are owned, you may enter `TSS PERMIT` commands to control access to those resources.

Step 5: Controlling Access to Product Resources

After a prefix has been added to the appropriate (owning) ACID to indicate that it is owned, the TSS PERMIT command can be used to permit end user access to resources with entity names beginning with the now-owned (defined) prefix.

Most resource entity names are entirely variable and can be customized at any level. You can establish `PERMITs` that control access to systems, products, view tables, and view action commands associated with a specific product resource, as shown in the following examples.

Example 1: To prohibit access to a resource universally, specify

```
TSS PERMIT(ALL) class(BBM.resource.name)              +
    ACCESS(NONE)
```

Example 2: To permit READ access by users connected to a profile, specify

```
TSS PERMIT(profile) class(BBM.resource.name)          +
    ACCESS(READ)
```

Example 3: To permit UPDATE access by the user whose ACID is BBMUSER, specify

```
TSS PERMIT(BBMUSER) class(BBM.resource.name)          +
    ACCESS(UPDATE)
```

Chapter 11. Class Definitions

Class definitions specify

- a class name transformation
- a prefix or suffix for resource entity names
- log options
- whether the class is active
- predefined authorization results
- access intent transformations
- CA-ACF2 or CA-TOP SECRET parameters

Class definitions are stored in BBMTSP*nn* members in the security parameter library. Refer to "Establishing Enhanced Security" on page 119 for details on this library and sharing a single library between CASs.

The following sections describe the Plex Manager views for managing class definitions.

Working with Class Definition Members

This section describes how to manage the class definition members in the security parameter library.

Displaying a List of Class Definition Members (SECDEFL)

To display a list of class definition members:

1. On the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. In the COMMAND line,enter **SECDEFL** . The SECDEFL view is displayed, as shown in Figure 13.

```
15JUL1998 12:43:14 ------------ INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
 W1 =SECDEFL===========SYSB=====*========15JUL1998==12:43:14====PLEXMGR=======3
CMD Member Description
--- Suffix ------------
    00     All Security Class Definitions
    01     Production Security Class Definitions
    02     SysA Test Security Class Definition
```

Figure 13. SECDEFL View

To display a class definition, enter the S line command in the **CMD** column. The SECDEF view is displayed. SECDEF is described in "Displaying a Class (SECDEF)" on page 147.

For a description of any SECDEFL field, place your cursor on the field and press your HELP PF key or see "Default Class Definitions" on page 337.

Note: If the security parameter library does not yet contain a class definition member, the **Description** field shows the following message:

```
Empty member--Select to create
```

Select the empty member using the S line command, which displays the following message:

```
BBMYA923E The parameter member BBMTSP00 is missing
```

Disregard the message and press ENTER. The SECDEF view is displayed with the default security classes.

Creating a Class Definition Member

Creating a new class definition member is useful if

- you need to change some of the security class parameters temporarily for a CAS
- CASs share a security parameter library, but one or more CASs require different class definitions

By creating a new class definition member in the security parameter library, you can retain your original definitions for use again or, in a shared security parameter library environment, provide more than one set of parameters for different system requirements.

To create a new class definition member:

1. Enter the SECDEFL command to display the SECDEFL view.
2. Review the list of member suffixes and choose a suffix that is not currently used.
3. In the COMMAND line, enter **`SECDEF SUFFIX(`*`nn`*`)`**, where *nn* is the suffix for the new member.
4. The following message is displayed:

   `BBMYA923E The parameter member BBMTSP`*`nn`*` is missing`

   Disregard the message and press ENTER to display the new member with the default security classes.
5. In the COMMAND line, enter **`EDIT`** and change a definition, as described in "Dynamically Activating Class Changes" on page 152.
6. In the COMMAND line, enter **`SAVE`**.

Activating a New Class Definition Member

If you want the CAS to use a new class definition member at initialization, you must identify the new member suffix in the CASDEF view.

1. From the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
1. Type **CASDEF** to display the CASDEF view.
2. In the COMMAND line, enter the **EDIT** command to obtain an edit lock.
3. In the COMMAND line, enter the **CHAnge** command.
4. Change the **SecDef Suffix** field in the CHANGE CAS SYSTEM DEFINITION dialog to the two-digit value of the class definition member you want the local CAS to use.
5. Press the END key to display the CASDEF view.
6. In the COMMAND line, enter the **SAVE** command to save the updated CAS definition in the BBPARM library.
7. In the COMMAND line, enter the **INStall** command to activate the CAS definition immediately for the local CAS to reference the new class definition member.

Deleting a Class Definition Member

To delete a class definition member from the security parameter library:

1. Enter the SECDEFL command to display the SECDEFL view.
2. In the COMMAND line, enter **EDIT**.
3. Type the DEL line command to the left of the member and press ENTER.

Note: The member is deleted immediately. There is no confirmation panel. Use this command only when you are sure you want to delete a security parameter library member.

Working with Class Definitions

This section describes how to manage the class definitions in a class definition member.

Displaying a Class (SECDEF)

To display the classes in the current class definition member:

1. From the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. Do one of the following:
   - On the EZSEC view, place your cursor on **Review Class Definitions** and press ENTER.

     or
   - In the COMMAND line, enter **SECDEF**.

The SECDEF view is displayed, as shown in Figure 14.

```
15JUL1998 12:43:40 ------------ INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
>W1 =SECDEF============SYSB=====*========(00 BROWSE        )====PLEXMGR======76
CMD SecClass NextClas Act Description                             Prefix
--- -------- -------- --- ------------                            ------------
    $BBM     FACILITY YES BBI-3 Default Resource Class
    $BOOLEL           YES Top Secret Sample User-defined RDT Class
    $BOOLES           YES Top Secret Sample User-defined RDT Class
    acf2RDSN DATASET  YES Redirect ACF2 TYPE(DSN) to ordinary rule
    ABSTRACT          YES Top Secret Validate User Resource Access
    ACICSPCT          YES CICS Program Control Table; Started Txns
    APPL              YES Application Access
    BCICSPCT          YES CICS Group Resource Class for ACICSPCT
    CCICSCMD          YES CICS System Programmer Commands
    CHGPROP           YES Top Secret Cross-CPU change propagation
    CPSMOBJ           YES CPSM Discrete and generic resources
    CPSMXMP           YES CPSM Exemption resource names
    DASDVOL           YES Top Secret Validate DASD volumes access
    DASDVOLT          YES Top Secret Validate ANY DASD vol. access
    DATASET           YES Data Set (Entity name = DSNAME)
    DATASETT          YES Top Secret Validate ANY data set access
```

Figure 14. SECDEF View

Each line in the SECDEF view represents one class definition in the class definition member in the security parameter library.

All known classes for CA-ACF2, CA-TOP SECRET, and RACF are displayed in the SECDEF view.

To display the attributes of a class listed in the SECDEF view, position the cursor on the class to display and press ENTER. The SECDEFD view is displayed as shown here.

```
27SEP1999  14:03:57 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
>W1 =SECDEF===SECDEFD==SJSB=====*========(00 BROWSE        )====PLEXMGR=======1
    Class Name..... $BBM       Description.. BBI-3 Default Resource Class
    NextClass...... FACILITY   Active....... YES
    Common.........
     Suffix........            Prefix.......
     ResList.......            Maxl.........
     LogFail.......            LogAuth......
    Intent Xform...
     Execute.......            Alter........
     Read..........            Create.......
     Update........            Write........
     Control.......            Delete.......
    TopSecret......
     Class.........            PrivPgm......
     List..........            DefProt......
     FastAuth......            ResMask......
     Auth..........            ClassMask....
```

Figure 15. SECDEFD View

Changing a Class

Important

Do not change a class definition unless you want to use a class name other than FACILITY.

All MAINVIEW products that operate in windows mode use the class name $BBM, which is translated automatically by MAINVIEW to the class name FACILITY. The FACILITY class is known to CA-ACF2, CA-TOP SECRET, and RACF.

To change a class definition, perform the following steps on each system in your sysplex or multisystem environment:

1. Start the CAS for which you want to change a class definition. If the security parameter library is shared by all CASs, you need only start one CAS.
2. From the MAINVIEW Selection Menu, select Option 0 for Parameters.
3. Specify the CAS for which you want to customize the member. After connecting to that CAS successfully, select Option 1 for Plex Manager.
4. In the COMMAND line, enter **SECDEF**.
5. In the COMMAND line, enter **EDIT** to obtain the edit lock for this member.
6. In the **CMD** column for the class you want to change, enter the C line command and press ENTER.

   The CHANGE SECURITY CLASS DEFINITION dialog, shown in Figure 16, is displayed.

```
---------------------- CHANGE SECURITY CLASS DEFINITION -------------------
 COMMAND ===>

Class Name  ===  $BBM     Next ===> FACILITY Active ===> YES
Description ===> BBI-3 Default Resource Class
Common:
  Prefix   ===>                              Suffix ===>
  Reslist  ===>        Yes/No Maxlen  ===>        CDT/STD/LONG/nn
  Log Fail ===>        Log Auth ===>        Never / Allow
Intent Transformations :    Intent / Yes / No / Maybe
  EXECUTE ===>           CONTROL ===>           WRITE  ===>
  READ    ===>           ALTER   ===>           DELETE ===>
  UPDATE  ===>           CREATE  ===>
TSS:  - This section applies only to systems using Top Secret
  Class   ===>           List ===>
  Fauth   ===>      Auth    ===>      PrivPgm   ===>      Yes/No
  DefProt ===>      ResMask ===>      ClassMask ===>      Yes/No
ACF2:   This section applies only to systems using ACF2
  Rule    ===>       List   ===>
  Resdir  ===>       Auth   ===>        Yes/No

Press End to change the security class definition.
```

Figure 16. CHANGE SECURITY CLASS DEFINITION Dialog

7. In the **Next** field, specify the class you want to use.

   For a description of an attribute, press the HELP PF key or see Table 47 on page 339.

8. Press the END key to display the SECDEF view.
9. In the COMMAND line, type the **SAVE** command. The SECURITY CLASS DEFINITION dialog is displayed, as shown in Figure 17

```
-------------------------- SECURITY CLASS DEFINITION ----------------------
COMMAND ===>

Security Class Member Description:
  ===> Default Security Classes

Enter END to save the security class definition parameter member.
Enter CANCEL to leave without saving.
```

Figure 17. SECURITY CLASS DEFINITION Dialog

Add or change the member description as necessary. The description can be up to 30 characters. It is displayed in the **Description** field of the SECDEFL view.

10. Press the END key to save class definition.

The member is saved in the security parameter library for the local CAS or, in a shared environment, for all CASs. Either the SECDEF or SECDEFD view is displayed and the edit-mode status field on the window information line changes from `(00 EDIT MOD  )` to `(00 EDIT     )`. Edit mode is still active and all modifications are saved.

This definition will be activated the next time the CAS initializes or immediately with the INSTall command (see "Dynamically Activating Class Changes" on page 152).

To cancel your changes, type the CANcel command on the COMMAND line. The class definition member will remain the way it was when the edit lock was obtained or since the last SAVE command was used.

Adding a New Class

To add a new class to the current class definition member:

1. From the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. In the COMMAND line, enter **SECDEF**.
3. In the COMMAND line, enter EDIT to obtain the edit lock for this member.
4. To create an empty class defintion, enter the ADD command in the COMMAND line.

   To use an existing class as a model, enter the A line command in the **CMD** column for that class and press ENTER.

   The ADD SECURITY CLASS DEFINITION dialog is displayed, as shown in Figure 18..

```
------------------------ ADD SECURITY CLASS DEFINITION --------------------
COMMAND ===>

Class Name  ===>          Next ===>          Active ===>
Description ===>
Common:
  Prefix   ===>                              Suffix ===>
  Reslist  ===>        Yes/No Maxlen  ===>        CDT/STD/LONG/nn
  Log Fail ===>        Log Auth ===>        Never / Allow
Intent Transformations :    Intent / Yes / No / Maybe
  EXECUTE ===>           CONTROL ===>           WRITE  ===>
  READ    ===>           ALTER   ===>           DELETE ===>
  UPDATE  ===>           CREATE  ===>
TSS:  - This section applies only to systems using Top Secret
  Class   ===>           List ===>
  Fauth   ===>      Auth    ===>      PrivPgm   ===>      Yes/No
  DefProt ===>      ResMask ===>      ClassMask ===>      Yes/No
ACF2:   This section applies only to systems using ACF2
  Rule    ===>       List   ===>
  Resdir  ===>       Auth   ===>        Yes/No

Press End to change the security class definition.
```

Figure 18. ADD SECURITY CLASS DEFINITION Dialog

   Provide the appropriate attributes for each security class.

   For a description of each parameter, press the HELP PF key. Table 47 on page 339 also describes each parameter.

   Press the END key to display the SECDEF view.

   In the COMMAND line, enter **SAVE** to save your default class definition member (suffix of 00) in the security parameter library.

5. To activate these default security class parameters, enter **INStall** in the COMMAND line. If each CAS has a unique security parameter library, repeat Step 2 through Step 5 on page 151 for each CAS.

If all CASs share the same security parameter library, start the other CASs. They will automatically use the parameters you customized in the default (suffix 00) member.

Note: If any of the CASs are not using the new security parameters in a shared security parameter library environment, see "Activating a New Class Definition Member" on page 147 to ensure that the 00 member is defined to each CAS.

To cancel your changes, type the CANcel command on the COMMAND line. The class definition member in the security parameter library retains its original contents when the edit lock was obtained or since the last SAVE command was used.

Deleting a Class

To delete a class from a class definition member:

1. From the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. In the COMMAND line, enter **SECDEF**.
3. In the COMMAND line, enter **EDIT** to obtain the edit lock for this member.
4. Enter the DEL line command in the **CMD** column for that class and press ENTER.

The security class is marked for deletion and removed from the display.

Recovering a Deleted Class

To recover a security class that was deleted from a class definition with the DEL line command, use the UND line command. The UND command recovers a definition that was deleted as long as the SAVE command has not been entered since the DEL command was used.

1. From the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. In the COMMAND line, enter **SECDEF**.
3. In the COMMAND line, enter **EDIT**.
4. Enter the following command in the COMMAND line:

   QPARm DELETED(*)

   This redisplays the classes marked for deletion.
5. Enter the UND line command to select the class name and press the ENTER key.

Note: Undeleting a class definition also changes the **Deleted?** field in the SECDEFD view from `No` to `Yes`.

Dynamically Activating Class Changes

To activate your changes immediately for the local CAS without waiting until the CAS is recycled or for the next system IPL, use the INSTall primary command from either the SECDEF or the SECDEFD view. You do not have to be in edit mode to use this command. Since the SECDEFD view displays only one security class from a class definition, only that member is activated.

For a shared security parameter library, you must display the class definition member in SECDEF and enter the INSTall command for each CAS.

Note: The INSTall command does not update a class definition member. You must use the SAVE command to update the class definition, as described in "Changing a Class" on page 149.

Chapter 12. Parameter Definitions

Parameter definitions control how MAINVIEW security interacts with your ESM. They

- specifiy the ESM and its attributes
- identify the MAINVIEW CAS subsystem to the ESM
- specify how the MAINVIEW security interface identifies MAINVIEW TS end users to the ESM within product address spaces
- activate diagnostic services

Parameter definitions are stored in the BBMTSS*nn* members in the security parameter library. Refer to "Establishing Enhanced Security" on page 119 for details on this library and sharing a single library between CASs.

The following sections describe the Plex Manager views for managing parameter definitions.

Displaying a List of Parameter Definitions (SEPDEFL)

The SEPDEFL view displays a list of the members in the security parameter library for the local CAS. To display SEPDEFL:

1. On the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. In the COMMAND line, enter **SEPDEFL**.

The SEPDEFL view is displayed, as shown in Figure 19.

```
15JUL1998 11:01:31 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                 SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
 W1 =SEPDEFL===========SYSC=====*========15JUL1998==11:01:30====PLEXMGR=======1
CMD Member Description
--- Suffix ------------
    00     Test System Security Parms
    01     Secondary Security Parms
```

Figure 19. SEPDEFL View

The **Member Suffix** column displays *nn*, where *nn* is suffix of the BBMTSS*nn* member.

The first time you display this view, the **Description** field shows the following message:

```
Empty member--Select to create
```

Selecting an empty member displays the following message in the SEPDEFD view:

```
BBMYA819E The parameter member BBMTSS00 is missing
```

Press ENTER; SEPDEFD shows the default security parameters.

Displaying a Parameter Definition (SEPDEF and SEPDEFD)

To display a parameter definition:

1. On the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. Do one of the following:
   - Type **EZSEC** to display the EZSEC view, place your cursor on **Review Security Parms**, and press ENTER.
   - Type **SEPDEFL** to display the SEPDEFL view and enter the S line command to the left of the parameter definition. The SEPDEFD view is displayed.
   - In the COMMAND line of a Plex Manager view, enter the following command:

SEPDEF SUFFIX(*nn*)

where *nn* is the two-digit suffix of the security parameter library member you want to display. The SEPDEF view is displayed.

The only difference between SEPDEF and SEPDEFD is the method by which you access them (by selection list or command); they display identical infomation, as shown here:

```
15JUL1998  09:06:22 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                 SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
>W1 =SEPDEFD===========SYSC=====*========(00 BROWSE        )====PLEXMGR=======1
    ESM Type....... AUTO     Base PRODUCT. BBI3
    ESM Attributes.
     EntityX....... YES      TSS PrivPgm.. STD
     DSType........ YES      TSS Messages. ALL
     ACF2 Messages. ALL
    SubSystem Id...
     Subsys Id..... SSID     Applid....... SSID
     ReqStor....... ASIS     Session Type. NONE
    End User Id....
     ESM Userid.... ACCEPT   Dflt Userid.. NONE
     Account Info.. ALLOW    Pgmr name.... ALLOW
     Dflt AcctInfo. EXTERNAL Acct Info Val *NONE*
     GROUP Inherit. ALLOW
    Diagnostics....
     Trace Value... OFF      Restart Limit   3
     Window Msgs... NONSAFE  Restart Time.  60
    Modification Id          Member Suffix 00
     UpdSystem..... SYSC     UpdTime...... 10:11:00
```

Figure 20. SEPDEFD View

Changing a Parameter Definition

Important

You do not need to change a parameter definition except for the following reasons:

- You have both CA-ACF2 and RACF and want to use RACF.
- You use the RACF GROUP feature, and do not want it inherited on a connected system. In this case, you must spsecify `IGNORE` for the `GROUP Inherit` option on the `CHANGE SECURITY PARAMETERS.`
- You use a security system other than RACF, CA-ACF2, or CA-Top Secret.

To change a parameter definition, your user ID must be authorized to update the security parameter library for each CAS on each MVS image.

To change the parameter definition for any of the reasons listed above:

1. Display the SEPDEF or SEPDEFD view using one of the methods described in "Displaying a Parameter Definition (SEPDEF and SEPDEFD)" on page 156.
2. Enter the EDIT command in the COMMAND line of the SEPDEF or SEPDEFD view. This locks the parameter definition and prevents others from updating it. The edit-mode

status field on the window information line changes from `(00 BROWSE  )` to `(00 EDIT )`.

3. Enter either **CHAnge** in the COMMAND line or the CH line command in the first column of the first row of data.

The CHANGE SECURITY PARAMETERS dialog is displayed, as shown in Figure 21.

```
------------------------- CHANGE SECURITY PARAMETERS ----------------------
COMMAND ===>

ESM Type           ===> AUTO
Base PRODUCT       ===> BBI3
ESM Attributes:
 Support EntityX   ===> YES         TSS Priv Program   ===> STD
 Support DSType=M  ===> YES         Display TSS Msgs   ===> ALL
 Display ACF2 Msgs ===> ALL
Subsystem Identification:
 Subsys ID         ===> SSID        Applid             ===> SSID
 Reqstor           ===> ASIS        Session type       ===> NONE
End User Identification:
 ESM Userid        ===> ACCEPT      Default Userid     ===> NONE
 Programmer name   ===> ALLOW       GROUP Inherit      ===> ALLOW
 Accouting Info    ===> ALLOW
  Default ===> EXTERNAL
Diagnostics and Trace:
 Security traces   ===> OFF         Security restart   ===> 3      times
 Window messages   ===> NONSAFE                   in   ===> 60     minutes

Press END to change the Security parms; CANCEL to leave without changing.
```

Figure 21. CHANGE SECURITY PARAMETERS Dialog

Overtype the parameters as necessary.

For a description of a parameter, position your cursor on the parameter field and press the HELP PF key (or see Table 46 on page 329).

You can cancel your changes at any time by entering CANcel in the COMMAND line. The current parameter definition is reinstated to its original contents when the edit mode was requested or since the last SAVE command was entered.

When your changes are complete, press your END PF key to return to the SEPDEF or SEPDEFD view.

Note: If you use the RACF GROUP feature, and do not want it inherited on a connected system, specify NO in the **GROUP Inherit** field on the CHANGE SECURITY PARAMETERS.

To save your change, enter the SAVE command in the COMMAND line of either the SEPDEF or SEPDEFD view while in edit mode. The SECURITY PARAMETERS DEFINITION dialog, shown in Figure 22, is displayed.

```
--------------------- SECURITY PARAMETERS DEFINITION -------------------
COMMAND ===>

Security Parameters Member Description:
  ===>

Enter END to save the security parameter definition member.
Enter CANCEL to leave without saving.
```

Figure 22. SECURITY PARAMETERS DEFINITION Dialog

If you are saving changes to an existing parameter definition, the previously defined description is shown. If you are creating a new parameter definition, this dialog appears with a blank **Member Description** field. The description can be changed and can be up to 30 characters in length. It is used in the **Description** field of the SECDEFL view.

Press your END PF key to save all your changes for this parameter definition as a member of the security parameter library. The member is saved in the security parameter library for the local CAS or, in a shared environment, for all CASs.

To make the parameter definition member known to the local CAS, see "Activating a Parameter Definition" on page 161. This definition is activated the next time the CAS initializes.

Creating a New Parameter Definition

To create a parameter definition, your user ID must be authorized to update the security parameter library for each CAS on each MVS system.

Use the following procedure to create a new parameter definition member:

1. Start MAINVIEW.
2. On the MAINVIEW Selection Menu, select Option 1 for Plex Manager. The PLEXOVER view is displayed.
3. In the COMMAND line, enter **`SEPDEF SUFFIX(`*`nn`*`)`** , where *nn* is the suffix for the BBMTSS*nn* member you want to create. Disregard the following message:

   `BBMYA819E The parameter member BBMTSS`*`nn`*` is missing`

   Press ENTER to display the SEPDEF view with the security parameters defined in the default member, BBMTSS00.
4. In the COMMAND line, enter **`EDIT`** to obtain the edit lock for this member.
5. In the COMMAND line, enter **`CHAnge`** to display the CHANGE SECURITY PARAMETERS dialog, as shown in Figure 21 on page 158.
6. Enter the appropriate information for each parameter you want to change. For a description of the parameters, press the HELP PF key or see Table 46 on page 329.
7. Press the END PF key to return to the SEPDEF view.
8. In the COMMAND line, enter **`SAVE`** to save the changes. The SECURITY PARAMETERS DEFINITION dialog is displayed. Type a description of the member in the **Description** field and press the END PF key to save the member. The new BBMTSS*nn* member will be saved in the security parameter library.
9. Follow the instructions in "Activating a Parameter Definition" on page 161 to associate the new parameter definition member to the CAS.

Activating a Parameter Definition

BBMTSS00 is the default parameter definition member in the security parameter library for a CAS. If you changed BBMTSS00, your changes will become effective when the CAS is recycled.

However, if you created a BBMTSS*nn* member with a suffix different from the default suffix of 00, you must associate the parameter definition suffix with the CAS, as described below. For example, if you created BBMTSS99, you must associate the suffix 99 to the CAS.

1. Display the CASDEF view.
2. Enter the EDIT command to obtain an edit lock.
3. Enter the CHA command to the left of the CAS definition you want to change.
4. Change the **SepDef Suffix** field on the CHANGE CAS SYSTEM DEFINITION dialog to the two-digit suffix of the parameter definition member you want the CAS to use.
5. Press the END PF key to return to the CASDEF view.
6. Enter the SAVE command in the COMMAND line to save the updated CAS definition in the BBPARM library.
7. Recycle the CAS.

Deleting a Parameter Definition

Note: When deleting a parameter definition, no confirmation panel is displayed. Use the DELete command only when you are sure you want to delete a security parameter library member.

To delete a parameter definition:

1. On the MAINVIEW Selection Menu, select Option 1 for Plex Manager.
2. In the COMMAND line, enter **SEPDEFL**.
3. In the SEPDEFL view, locate the parameter definition.
4. Enter the DEL line command to the left of the parameter definition.

Chapter 13. Resource Definitions

This chapter assumes that you have read Chapter 9, “Introduction to Enhanced Security”.

Before You Begin

Perform the following steps before you begin customizing your resource definition members:

1. Determine if you even need to create a resource definition member.

   If your ESM can work with the MAINVIEW security interface using default security resource parameters as distributed, you do not need to create a new definition. Or, your ESM may require only a few changes to some of the attributes for some of the resources.

2. Ensure that your user ID is authorized to access each CAS on each MVS.

3. Ensure that your user ID is authorized to access the security parameter library for each CAS on each MVS.

4. Optionally, determine the resource class and entity names for resources already known to your ESM if these resources have the proper security attributes you want to use to control access to resources.

5. Ensure that the CAS and each PAS are properly authorized for your ESM, as described in Chapter 10, “Configuring Your ESM for Enhanced Security”.

??You must complete the steps in this section to control access to MAINVIEW products. These products run with security by default...??

Working with Resource Definition Members

This section describes how to manage resource definition members in the security parameter library.

Displaying a List of Members using the SERDEFL View

To display a list of resource definition members in the security parameter library:

1. From the MAINVIEW Selection Menu, select the product for which you want to display the members.
2. In the COMMAND line, enter **SERDEFL**.

The SERDEFL view is displayed. A sample SERDEFL for Plex Manager is displayed in Figure 23.

```
15JUL1998 18:38:51 ------------ INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                  SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
 W1 =SERDEFL===========SYSB=====*========15JUL1998==18:38:51====PLEXMGR=======2
CMD Product  Member Description
--- -------- Suffix ------------
    COMMON   00     Common Resources
    PLEXMGR  00     Plex Manager Resources
```

Figure 23. SERDEFL View in Plex Manager

Use the SERDEFL view to

- select a member for display in the SERDEF view
- delete a resource definition member from the security parameter library, as described in "Deleting a Member" on page 166

To display help for any SERDEFL field, place your cursor on the field and press your HELP PF key.

Creating a New Resource Definition Member

You may need to change some of the security resource parameters temporarily for a CAS or, for a shared security parameter library environment, you may have one or more CASs that require different security resource parameters. By creating a new resource definition member in the security parameter library, you can retain your original parameters for use again or, in a shared security parameter library environment, provide more than one set of parameters for different system requirements.

To create a new resource definition member in the security parameter library, use the following command:

```
SERDEF SUFFIX(nn)
```

where *nn* is a two-digit numeric suffix (00 to 99) identifying the new member. The suffix must not be in use already (use the SERDEFL view to display the suffixes already used by existing members).

The SERDEF view is displayed.

To make the new resource definition member known to the local CAS, see:

- "Activating a New Member for Common Resources"
- "Activating a New Member for Product Resources"

Activating a New Member for Common Resources

To activate a resource definition member of the security parameter library for the local CAS to use at initialization, the member needs to be identified to the CAS. If you updated the default (suffix 00) member, you do not need to change the CAS definition, as described below.

1. From Plex Manager, display the CASDEF view.
2. In the COMMAND line, enter **`EDIT`** to obtain the edit lock.
3. In the COMMAND line, enter **`CHAnge`**.
4. Change the **Common Serdef** field in the CHANGE CAS SYSTEM DEFINITION dialog to the two-digit value of the resource definition member you want the local CAS to use for common MAINVIEW resources.
5. Press the END key to display the CASDEF view.
6. In the COMMAND line, enter **`SAVE`** to save the updated CAS definition in the BBPARM library.
7. In the COMMAND line, enter **`INStall`** to activate the CAS definition immediately for the local CAS to reference the new resource definition member for common MAINVIEW resources.

Activating a New Member for Product Resources

To activate a new resource definition member of the security parameter library for a product, the target definition for that product must reference the new resource definition member.

To verify or update the resource definition being used by a product:

1. From Plex Manager, display the CASDEF view.
2. Select the CAS for the product with your cursor and press the ENTER key to display the CASDEFD view.
3. Review the **TgtDef Suffix in the Parmlib Suffixes** section of this view.
4. Display the TGTDEFL view in Plex Manager, as described in the *MAINVIEW Administration Guide*.
5. Select the member that has the same suffix as the CASDEFD **TgtDef Suffix** field to display the TGTDEF view.

6. Scan the list of product targets to identify the target that is to reference the new resource definition.
7. Select the CAS for the product with your cursor and press the ENTER key to display the TGTDEFD view.
8. Verify the suffix value in the **SerDef Suffix** field of the **Security Info** section in TGTDEFD.

   If this value is the same as the new resource definition member, the target definition does not need to be edited. If this value is not the same as the new resource definition member, edit the target definition to specify the suffix of the new member.
9. Enter the SAVE command to save the target definition in the BBPARM library.
10. Recycle the CAS and the PAS, as described in the *MAINVIEW Administration Guide*.

Deleting a Member

To delete a resource definition member:

1. In the COMMAND line of the SERDEFL view, enter **`EDIT`**.
2. Select the definition you want to remove from the security parameter library with the DEL line command.

No confirmation panel is displayed when you delete a resource definition member. Use this command only when you are sure you want to delete a security parameter library member.

Working with Resource Definitions

The views for managing resource definitions are as follows:

EZSECRES Is an extension of EZSEC that allows you to change the context or product before displaying product resources.

SERDEFP Lists the active products for the current context when hyperlinking from EZSECRES.

SERDEFC Lists the active targets for the product selected by hyperlinking from SERDEFP when hyperlinking from EZSECRES.

SERDEFOV Displays group resource definitions categories of resources for the current product and context.

SERDEFEX Lists the components of the category selected by hyperlinking from the +++ value in the **Exp** column in SERDEFOV.

SERDEFL Lists all the resource definition members. You can select a member for display or delete a member.

SERDEF Displays both group and individual resource definitions. Use this view to create, change, enable, or disable a resource definition.

On the EZSEC view, hyperlink from the **Common Resources** field to display the SERDEFOV view, as shown in Figure 24.

```
04JAN2000  13:40:19 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                  SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
>W1 =SERDEFOV==========CXTSTJ===*========(00 BROWSE        )====PLEXMGR======12
CMD Description                              Enab Exp Change Comment
--- ------------                             ---- --- --------------
    Default - Table Data                     Yes  +++
    Default - Any Table Actions              Yes  +++
    Default - Alter Data Set                 No   +++
    Default - Specific Table Actions         Yes  +++
    Any Action (COMMON Views)                Yes  N/A
    Global - Connect to CAS                  Yes  N/A
    Global - Attach Product Service Point    Yes  N/A
    Global - Determine trusted status        No   N/A
    Global - Access a Product                Yes  N/A
    Global - Set Threshold - Save Central    Yes  N/A
    Enter ASU Mode                           Yes  N/A
    Customize a View                         Yes  N/A
```

Figure 24. SERDEFOV View

The SERDEFOV view lists each resource definition for the current context and product and indicates whether it is enabled.

Three plus signs (+++) in the **Exp** column indicate a default resource definition, which controls several individual resource definitions. If you change, enable, or disable a default resource definition, all the individual resource definitions that reference the default definition are changed, enabled, or disabled.

To display the individual resource definitions in a group, position the cursor on the +++ in the **Exp** column and press ENTER. The SERDEFEX view is displayed, as shown in Figure 25.

```
04JAN2000  13:42:20 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
>W1 =SERDEFOV=SERDEFEX=CXTSTJ===*========(00 BROWSE        )====PLEXMGR=======7
CMD Description                              Enab Change Comment
--- ------------                             ---- --------------
    Menu - Table Data                        No
    Screens - Table Data                     No
    Views - Table Data                       No
    Hist Data Set List - Table Data          Yes
    Security Resources - Table Data          Yes
    SecResource List - Table Data            Yes
    Diagmsg - Table Data                     Yes
```

Figure 25. SERDEFEX View

You can browse, enable, disable, and change resource definitions using the SERDEFOV and SERDEFEX views, as explained in the following sections.

Browsing a Resource Definition

To display a resource definition in browse mode from the SERDEFOV or SERDEFEX view, position the cursor on the **Description** column and press the ENTER key. The attributes of the resource definition are displayed by the SERDEFE view.

```
04JAN2000  13:44:08 ----------- INFORMATION DISPLAY ---------------------------
COMMAND  ===>                                                SCROLL ===> CSR
CURR WIN ===> 1        ALT WIN ===>
>W1 =SERDEFOV=SERDEFE==CXTSTJ===*========(00 BROWSE        )====PLEXMGR=======1
    Res Key..... BBC3X100     Desc..... Menu - Table Data
     Enabled.... No           Comment.. *Unchanged*
                              Type..... VIEW
    ESM Info---.
     Class...... $BBM         Entity... BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD
     VolSer..... *NONE*       Intent... READ
     LogAuth.... Allow        LogFail.. Allow
    Substitution Values
     IntTable... MX100        ExtTable. @Menu
     IntAction.. VIEWTAB      ExtAction VIEW
     IntActTab.. BBMTH0P0     Product.. COMMON
     Parms?..... No           Fields?.. Yes
    Update Info.              Mem Suff. 00
     UpdSystem.. *NONE*       UpdTime.. 13:41:04
     UpdUser.... *NONE*       UpdDate.. 04JAN2000
    Res Version.
     Version.... 3            Release.. 2
                              ModLevel. 0
```

Figure 26. SERDEFE View

The window information line indicates that you are in `BROWSE` mode.

For an explanation of any field in this view, place your cursor on the field and press your HELP PF key. Use PF3 to return to previous view.

The SERDEF view displays the entity name for the resource in the **Entity** field. The variable portions of the entity name are symbolics, which begin with an ampersand. The values that are substituted for those symbolics are displayed in the **Substitution Values** field. When creating a rule, profile, or permit to control access to a resource, the substitued values (or generic values) must be specified in the entity name, not the symbolics.

Enabling a Resource Definition

To enable a resource definition from the SERDEFOV or SERDEFEX view:

1. In the COMMAND line, enter **`EDIT`** to obtain an edit lock.
2. Type the E line command to the left of the resource definition you want to enable and press ENTER.
3. In the COMMAND line, enter **`SAVE`** to save the changes to the BBSECURE member.

Once the resource definition is enabled, access authorization requests can be made to your ESM for that resource.

Disabling a Resource Definition

To disable a resource definition from the SERDEFOV or SERDEFEX view:

1. In the COMMAND line, enter **`EDIT`** to obtain an edit lock.
2. Type the DIS line command to the left of the resource definition you want to enable and press ENTER.
3. In the COMMAND line, enter **`SAVE`** to save the changes to the BBSECURE member.

Changing a Resource Definition

To change the class, entity name, access intent, and log options of a resource definition using the SERDEFOV or SERDEFEX view:

1. In the COMMAND line, enter **`EDIT`** to obtain the edit lock for this member.
2. Type the C line command to the left of the resource definition you want to enable and press ENTER.

   The CHANGE RESOURCE AUTHORIZATION DEFINITION dialog, shown in Figure 27 on page 170, is displayed.

```
------------------ CHANGE RESOURCE AUTHORIZATION DEFINITION ---------------
COMMAND ===>

Authorize ===  CAS Definitions - Table Data
Product   ===  PLEXMGR          Type             ===  VIEW
Object    ===  CasDefn          Internal Object  ===  BBMTH0P0
Action    ===  VIEW             Internal Action  ===  VIEWTAB
Fields    ===  Y                Status           ===  Enabled
Parms     ===                  -
          ===                  -
          ===                  -
          ===                  -

Class   ===> $BBM
EntName ===> BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD
        ===>
        ===>
Intent  ===> READ
LogAuth ===> A        LogFail ===> A         (A - Allow, N - Never)
Comment ===> TEST

Press End to change the resource authorization definition.
```

Figure 27. CHANGE RESOURCE AUTHORIZATION DEFINITION Dialog

You can change the entity name, class name, access intent, logging attributes, and comment.

3. Specify the appropriate attributes for each parameter you want to change.

   You can use the CANcel primary command at any time.

   For a description of a parameter, press the HELP PF key.

4. Press the END key to return to the SERDEF view.

5. In the COMMAND line, enter **SAVE** to save your default resource definition member (suffix of 00) in the security parameter library.

6. Recycle the CAS, and the PAS if necessary, to activate your changes.

7. If each CAS and PAS has a unique security parameter library, repeat these steps for each appropriate CAS and product PAS.

   If all CASs and PASs share the same security parameter library, start the other CASs and PASs. They will automatically use the definitions you customized in the default member (suffix 00).

   Note: If any of the CASs or PASs are not using the new resource definition in a shared security parameter library environment:

   - See "Activating a New Member for Common Resources" on page 165 to ensure that the 00 member is defined to each CAS for common resources.
   - See "Activating a New Member for Product Resources" on page 165 to ensure that the 00 member is defined to each CAS for product-specific resources.

Once you have changed a resource definition, you can

- cancel your changes with the CANcel primary command, as described in "Canceling Resource Definition Changes"

- save the resource definition changes in the security parameter library member using the SAVE primary command, as described in "Saving a Resource Definition" on page 171

Canceling Resource Definition Changes

To cancel changes that you made in edit mode since the last time SAVE was entered, enter CANcel in the COMMAND line of any of the security views.

If you use CANcel when the CHANGE RESOURCE AUTHORIZATION DEFINITION dialog is displayed, the SERDEF view appears and the edit lock is still active.

If you use CANcel when the SERDEF, SERDEFE, or SERDEFD view is displayed, the edit-mode status field on the window information line changes from `EDIT` to `BROWSE` to indicate that the edit lock is no longer active.

The resource definition member in the security parameter library retains its original contents when the edit lock was obtained or since the last SAVE command was used.

Saving a Resource Definition

To save changes to a resource definition, enter **`SAVE`** in the COMMAND line of either the SERDEF or SERDEFE/SERDEFD view in edit mode. The following dialog is displayed:

```
---------------- SECURITY RESOURCE DEFINITION PARAMETER MEMBER ------------
COMMAND ===>

Security Resource Member Description:
  ===> Plex Manager Resources

Enter END to save the resource definition parameter member.
Enter CANCEL to leave without saving.
```

Figure 28. SECURITY RESOURCE DEFINITION PARAMETER MEMBER Dialog

If you are saving changes to an existing resource definition, the previously defined description is shown. If you are saving a new resource definition, the **Member Description** field is blank. The description can be changed and can be up to 30 characters in length. It is used in the **Description** field of the SERDEFL view.

Pressing your END key saves all your changes for this resource definition as a member of the security parameter library. The member is saved in the security parameter library for the local CAS or, in a shared environment, for all CASs. To make the resource definition member known to the local CAS, see

- "Activating a New Member for Common Resources" on page 165
- "Activating a New Member for Product Resources" on page 165

Chapter 14. Protecting the MAINVIEW Security Interface

To control unauthorized changes to your security environment, you must restrict access to resources that protect the MAINVIEW security interface. To do this, you should define a permit, profile, or rule to prohibit universal access to the views used to implement and maintain security parameter and resource access definitions. By not allowing users to access these views, you effectively prevent unauthorized changes from being made.

To restrict access to security views:

1. Access the COMMON resource member from the Plex Manager SERDEFL view and secure the following resources:
   - `Security Resources - Table Data` (for SERDEF, SERDEFD, and SERDEFE views)
   - `SecResource List - Table Data` (for SERDEFL view)
2. Access the PLEXMGR resource member from the Plex Manager SERDEFL view and secure the following resources:
   - `SecDef Security Class - Table Data` (for SECDEF and SECDEFD views)
   - `SecDef List - Table Data` (for SECDEFL view)
   - `SecParm Definitions - Table Data` (for SEPDEF and SEPDEFD views)
   - `SecParm Def List - Table Data` (for SEPDEFL view)

Chapter 15. Resources Definitions Listed by Product

Each MAINVIEW product is shipped with resource defintions for

- resources common to all MAINVIEW products
- resources specific to a product, such as data accessed by views and forms, commands (product or view actions), and line commands (actions against objects or elements displayed in a view)

Protected resources are identified to your ESM by a resource name.

The SERDEFL view lists resource definition members that reside in a security parameter library, called BBSECURE by default. Selecting a definition from SERDEFL shows a description of each resource as modified, if necessary, in that definition in the SERDEF view. The MAINVIEW security interface uses the information from this view to build the authorization request it makes to your ESM. These authorization requests for common and product-specific resources are shown in the tables starting on page 175 by

- type of default resource viewed with SERDEF
- type of authorization request passed to your ESM

Common MAINVIEW Resources

To disable, enable, or customize resource access authorization requests to your ESM for a common resource used by all MAINVIEW products:

1. Display the SERDEFL view in Plex Manager, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the `COMMON` resource definition.

To enable or disable security for all common resources, you only need to disable or enable all of the following high-level resources, as described in "Disabling a Resource Definition" on page 169.

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Actions
- Any Action (Common Views)
- Global - Connect to CAS
- Global - Attach Product Service Point
- Global - Determine trusted status
- Global - Access a Product
- Global - Set Threshold - Save Central
- Enter ASU Mode
- Customize a View

Authorization requests for resources common to MAINVIEW products are built from the default entity name for the `COMMON` resource definition as shown in Table 13 below. For a description of how the symbolics are used, see page 111.

Table 13. Resource Definitions Common to All MAINVIEW Products

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access data for a view in the current product? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid.tableid.*OD Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Default - Any Table Actions	Can the user enter a view action in a view in the current product? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.*productid.targetid.tableid.*AO Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Default - Alter Data Set	Can the user access a data set? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • Security Resources - Action - Edit • SecResource List - Action - Delete This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Class Name:** DATASET **Entity Name:** &DSN Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.

Table 13. Resource Definitions Common to All MAINVIEW Products (Continued)

Description of resource in SERDEF view	Resource name
Default - Set Threshold - Alter Data Set	Can the user access the data set containing threshold definitions? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, through the Customize a View view. **Class Name:** DATASET **Entity Name:** &DSN
Default - Specific Table Actions	Can the user enter specific view actions in the DIAGMSG, SERDEFL, or SERDEF views? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.tableid.actionid.*OA Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Any Action (Common Views)	Can the user enter view actions in the VIEWS or SCREENS views in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.COMMON.AA **Entity Name after Substitution:** BBM.*productid.targetid.*COMMON.AA
Global - Connect to CAS	Can the user connect to a CAS? **Default Entity Name:** BBM.&SSID.CN **Entity Name after Substitution:** BBM.*ssid.*CN
Global - Attach Product Service Point	Is this address space allowed to define itself as a product? **Default Entity Name:** BBM.&SYSTEM.&PRODUCT.&CONTEXT.TC **Entity Name after Substitution:** BBM.*systemid.productid.targetid.*TC

Table 13. Resource Definitions Common to All MAINVIEW Products (Continued)

Description of resource in SERDEF view	Resource name
Global - Determine trusted status	Is the remote PAS a trusted system? Any user in any address space in a system, whether or not they are previously connected to a CAS, can request data, services, or both from certain products when an appropriate interface is provided. In most circumstances, the system's external security manager (ESM) authorizes requested access to these product resources. This resource definition is used by products to determine if it is permitted, under certain, well-defined circumstances, to grant access to data, services or both to users signed on to a trusted system without specifically authorizing such access to each user. The distributed default is disabled; all PASs on all systems are trusted. This is usually the case in the majority of instances where the only service points available to a given user are just those on interconnected, trusted systems controlled by a single organization. In these instances, any user in any address space on any system can access only certain product resources (those subject to the trusted system origination test) without having to explicitly sign on to the product or be individually authorized for access. This resource definition can be enabled on a system where there are remote systems (targets) defined in the sysplex that are not trusted. Each remote PAS's trusted status is determined once at each local system. If the remote PAS's user ID has access to this resource on the local system, it is trusted. Any user signed on to a nontrusted system is handled in the usual way rather than the trusted system “fast path” exclusion from normal security system authorization. A nontrusted system user requesting access to certain product resources has an ESM security environment created for them locally. It must then be determined if the requesting user has the right to be granted access to the data or services provided by the product under well-defined circumstances. **Default Entity Name:** BBM.&SYSTEM.&PRODUCT.&CONTEXT.TS **Entity Name after Substitution:** BBM.*systemid.productid.targetid.*TS
Global - Access a Product	Can the user access this product on this system? **Default Entity Name:** BBM.&SYSTEM.&PRODUCT.&CONTEXT.TA **Entity Name after Substitution:** BBM.*systemid.productid.targetid.*TA
Global - Set Threshold - Save Central	Can the user save a threshold to a central place? **Default Entity Name:** BBM.&SYSTEM.&PRODUCT.&CONTEXT.TH **Entity Name after Substitution:** BBM.*systemid.productid.targetid.*TH
Enter ASU Mode	Can the user enter the ASU command to place that terminal session in automatic update mode? **Default Entity Name:** BBM.COMMON.ASU.PA
Customize a View	Can the user enter the CUSTom command to access view customization in any product? **Default Entity Name:** BBM.COMMON.CUSTOM.PA

Table 13. Resource Definitions Common to All MAINVIEW Products (Continued)

Description of resource in SERDEF view	Resource name
Diagmsg Table Data	Can the user access the DIAGMSG view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid.*MYA40.OD
Diagmsg - Any Action	Can the user enter a view action in the DIAGMSG view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.*productid.targetid.*MYA40.AO
Diagmsg - Action - On	Can the user enter the ON command in the DIAGMSG view in the current product to enable a diagnostic messaging option? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.MYA40.#MSGSDAID.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYA40.*value*OA where *value* represents what is actually displayed in the Option column of the DIAGMSG view.
Diagmsg - Action - Off	Can the user enter the OFF command in the DIAGMSG view in the current product to disable a diagnostic messaging option? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.MYA40.#MSGSDAID.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYA40.*value.*OA where *value* represents what is actually displayed in the Option column of the DIAGMSG view.
Diagnostic Storage - Table Data	Can the user access the DIAGSTOR view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid.*MVA50.OD **Note:** The DIAGSTOR view displays storage available to the PAS, any key, LSQA, SQA, and CSA. DIAGSTOR should be used only at the request of BMC Software Customer Support and should be protected from unauthorized access.
Hist Data Set List - Table Data	Can the user access data for the DSLIST view in the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.OD
Hist Data Set List - Any Action	Can the user enter a DSLIST view action in the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.*producidcontextid.*MYAG0.AO
Hist Data Set List - Action - Unquiesce	Can the user enter the U command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.UNQUIESC.OA

Table 13. Resource Definitions Common to All MAINVIEW Products (Continued)

Description of resource in SERDEF view	Resource name
Hist Data Set List - Action - Dealloc	Can the user enter the D command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.UNALLOC.OA
Hist Data Set List - Action - Save	Can the user enter the SAVE command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.SAVE.OA
Hist Data Set List - Action - Reset	Can the user enter the R command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.RESET.OA
Hist Data Set List - Action - Quiesce	Can the user enter the Q command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.QUIESCE.OA
Hist Data Set List - Action - Force	Can the user enter the F command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.FORCE.OA
Hist Data Set List - Action - Order	Can the user enter the O command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.CHANGE.OA
Hist Data Set List - Action - Add	Can the user enter the ADD command in the DSLIST view for the current MAINVIEW product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid.*MYAG0.ADD.OA
Menu - Table Data	Can the user access an EZMenu in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid.*MX100.OD

Table 13. Resource Definitions Common to All MAINVIEW Products (Continued)

Description of resource in SERDEF view	Resource name
Screens - Table Data	Can the user access the SCREENS view in the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, through any security call made to ask if you can access the data in a view. If you select a screen definition that references data you are not permitted to access, the window is opened for the view but no data appears. An error message is displayed that states you are not authorized to display the view data. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid*.MCE90.OD
Security Resources - Table Data	Can the user access the SERDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid*.MYA20.OD
Security Resources - Any Action	Can the user enter a view action in the SERDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.*productid.targetid*.MYA20.AO
Security Resources - Action - Edit	Can the user enter the EDIT command in the SERDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid*.MYA20.EDIT.OA
Security Resources - Alter Data Set	Can the user access the data set containing security resource parameter members? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • Security Resources - Action - Edit **Class Name:** DATASET **Entity Name:** &DSN
SecResource List - Table Data	Can the user access the SERDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid*.MYA30.OD
SecResource List - Any Action	Can the user enter a view action in the SERDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.*productid.targetid*.MYA30.AO

Table 13. Resource Definitions Common to All MAINVIEW Products (Continued)

Description of resource in SERDEF view	Resource name
SecResource List - Action - Delete	Can the user enter the DELete command in the SERDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.*productid.targetid*.MYA30.DELETE.OA
SecResource List - Alter Data Set	Can the user access the data set containing security resource parameter members? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SecResource List - Action - Delete **Class Name:** DATASET **Entity Name:** &DSN
Views - Table Data	Can the user access the VIEWS view in the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, through any security call made to ask if you can access the data associated with a specific view. If you select a view that references data you are not permitted to access, an error message is displayed that states you are not authorized to display the view data. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.*productid.targetid*.MCE95.OD

Plex Manager Resources

To disable, enable, or customize resource access authorization requests to the ESM for a Plex Manager security resource:

1. Display the SERDEFL view in Plex Manager, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `PLEXMGR`.

A total of five unique entity names control all Plex Manager resources. To enable or disable all security for Plex Manager, you need only disable or enable all of the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Actions
- Any Action (Plex Manager Views)

The following table lists all the security resources that are protected by Plex Manager. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 14. Resource Definitions for Plex Manager

Description of resource in SERDEF view	Resource name
Default - Table Data	Can the user access data for a Plex Manager view in the current product? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid.tableid.*OD Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Default - Any Table Actions	Can the user enter a view action for the current Plex Manager view? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid.tableid.*AO Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
Default - Alter Data Set	Can the user access a data set? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • CAS Definitions - Alter Data Set • SecDef Security Class - Alter Data Set • SecDef List - Alter Data Set • SecParm Definitions - Alter Data Set • SecParm Def List - Alter Data Set • SSI Context Defs - Alter Data Set • SSI Context Def List - Alter Data Set • Target Definitions - Alter Data Set • Target Def List - Alter Data Set This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following class name. **Class Name:** DATASET **Entity Name:** &DSN Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Default - Specific Table Action	Can the user enter specific view actions in the CASDEF, SECDEF, SECDEFL, SEPDEF, SEPDEFL, CONDEF, CONDEFL, TGTDEF, or TGTDEFL views in the current Plex Manager product? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.*tableid*.*actionid*.OA Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Any Action (Plexmgr Views)	Can the user enter a view action in the current Plex Manager product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.AA
CAS Active - Table Data	Can the user access data for the CASACT view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAD0.OD

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
CAS Active - Any Action	Can the user enter a view action in the CASACT view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAD0.AO
CAS Definitions - Table Data	Can the user access data for the CASDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAB0.OD
CAS Definitions - Any Action	Can the user enter a view action in the CASDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAB0.AO
CAS Definitions - Action - Install	Can the user enter the INStall command in the CASDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAB0.INSTALL.OA
CAS Definitions - Action - Edit	Can the user enter the EDIT command in the CASDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAB0.EDIT.OA
CAS Definitions - Alter Data Set	Can the user access the BBPARM data set where CAS definitions reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • CAS Definitions - Action - Edit **Class Name:** DATASET **Entity Name:** &DSN
Plex - Table Data	Can the user access the PLEX, PLEXOVER, TGTACT, and TGTACTZ views in the current product? **Note:** The PLEXOVER view is the default view that displays upon access to Plex Manager. An error results for any user who is denied access to this resource through the ESM. You can create a screen definition containing an acceptable view and name it PLEXMGR to avoid error messages occuring for these users when accessing Plex Manager. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CCE92.OD

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
SecDef Security Class - Table Data	Can the user access the SECDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA90.OD
SecDef Security Class - Any Action	Can the user enter a view action in the SECDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA90.AO
SecDef Security Class - Action - Edit	Can the user enter the EDIT command in the SECDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA90.EDIT.OA
SecDef Security Class - Alter Data Set	Can the user access the security parameter library where definitions for security class resource properties reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SecDef Security Class - Action - Edit **Class Name:** DATASET **Entity Name:** &DSN
SecDef List - Table Data	Can the user access the SECDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAA0.OD
SecDef List - Any Action	Can the user enter a view action in the SECDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAA0.AO
SecDef List - Action - Delete	Can the user enter the DELete command in the SECDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAA0.DELETE.OA

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
SecDef List - Alter Data Set	Can the user access the security parameter library where definitions for security class resource properties reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SecDef List - Action - Delete **Class Name:** DATASET **Entity Name:** &DSN
SecParm Definitions - Table Data	Can the user access the SEPDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA80.OD
SecParm Definitions - Any Action	Can the user enter a view action in the SEPDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA80.AO
SecParm Definitions - Action - Edit	Can the user enter the EDIT command in the SEPDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA80.EDIT.OA
SecParm Definitions - Alter Data Set	Can the user access the security parameter librarysecurity parameter library where definitions for global security parameters reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SecParm Definitions - Action - Edit **Class Name:** DATASET **Entity Name:** &DSN
SecParm Def List - Table Data	Can the user access the SEPDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAE0.OD
SecParm Def List - Any Action	Can the user enter a view action in the SEPDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAE0.AO

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
SecParm Def List - Action - Delete	Can the user enter the DELete command in the SEPDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAE0.DELETE.OA
SecParm Def List - Alter Data Set	Can the user access the security parameter library where definitions for global security parameters reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SecParm Def List - Action - Delete **Class Name:** DATASET **Entity Name:** &DSN
DiagSess - BBC Sessions - Table Data	Can the user access the DIAGSESS view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CZZ02.OD
SSI Context Defs - Table Data	Can the user access the CONDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA50.OD
SSI Context Defs - Any Action	Can the user enter a view action in the CONDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA50.AO
SSI Context Defs - Action - Install	Can the user enter the INSTall command in the CONDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA50.INSTALL.OA
SSI Context Defs - Action - Edit	Can the user enter the EDIT command in the CONDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA50.EDIT.OA

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
SSI Context Defs - Alter Data Set	Can the user access the BBPARM data set where SSI context definitions reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SSI Context Defs - Action - Edit **Class Name:** DATASET **Entity Name:** &DSN
SSI Context Def List - Table Data	Can the user access the CONDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA60.OD
SSI Context Def List - Any Action	Can the user enter a view action in the CONDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA60.AO
SSI Context Def List - Action - Delete	Can the user enter the DELete command in the CONDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA60.DELETE.OA
SSI Context Def List - Alter Data Set	Can the user access the BBPARM data set where SSI context definitions reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • SSI Context Def List - Action - Delete **Class Name:** DATASET **Entity Name:** &DSN
SSIContextMem - Table Data	Can the user access the CONACT, CONACTZ, or CONACTD views in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA70.OD
DiagSys - BBC Systems - Table Data	Can the user access the DIAGSYS view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CZZ01.OD

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
Target Definitions - Table Data	Can the user access the TGTDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA10.OD
Target Definitions - Any Action	Can the user enter a view action in the TGTDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA10.AO
Target Definitions - Action - Install	Can the user enter the INSTall command in the TGTDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA10.INSTALL.OA
Target Definitions - Action - Edit	Can the user enter the EDIT command in the TGTDEF view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYA10.EDIT.OA
Target Definitions - Alter Data Set	Can the user access the BBPARM data set where target definitions reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • Target Definitions - Action - Edit **Class Name:** DATASET **Entity Name:** &DSN
Target Def List - Table Data	Can the user access the TGTDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAC0.OD
Target Def List - Any Action	Can the user enter a view action in the TGTDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAC0.AO

Table 14. Resource Definitions for Plex Manager (Continued)

Description of resource in SERDEF view	Resource name
Target Def List - Action - Delete	Can the user enter the DELete command in the TGTDEFL view in the current product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.PLEXMGR.*targetid*.CYAC0.DELETE.OA
Target Def List - Alter Data Set	Can the user access the BBPARM data set where target definitions reside for the current product? **Note:** This resource is distributed as a disabled, rather than an enabled, security call because the security check is done, by default, at a more precise level through the following common resources: • Default - Any Table Actions • Default - Specific Table Actions • Target Def List - Action - Delete **Class Name:** DATASET **Entity Name:** &DSN

CMF MONITOR and MAINVIEW for OS/390 Resources

To disable, enable, or customize resource access authorization requests to the ESM for resources accessed through the MVS PAS:

1. Display the SERDEFL view in either or both CMF MONITOR or MAINVIEW for OS/390 (for whichever product you are customizing) as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change.

Note: If you have both products and want the security calls made for each product to be different, you can

1. customize one set of calls in the default member (suffix 00)
2. customize another set of calls in a member with a suffix value of 01 (or any two-digit value up to 99)
3. define target definitions for each product that specify the appropriate suffix value in the **SerDef Suffix** field

A total of five unique entity names control all CMF MONITOR and MAINVIEW for OS/390 resources. To enable or disable all security for these two products, you need only disable or enable all of the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Primary Actions (All Views)
- Default - Specific Table Actions
- Any Action (MVMVS or CMF Views)

Note: The MVScope facility can collect and display data accessed by I/O requests. This data can be displayed in the MSICCW view. Because of the sensitive nature of some of the data collected, by default the MAINVIEW Security Interface prevents users from collecting or viewing I/O data. To allow all users access to I/O data, disable the security for `MVMVS MVScope provide I/O data` in the SERDEF view. To allow specific users to collect and view I/O data, follow the procedures specified by your ESM for that resource.

The following table lists all the resources that are protected by CMF MONITOR and MAINVIEW for OS/390. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390

Description of resource in SERDEF view	Resource name
Default - Table Data	Can the user access a view in CMF MONITOR, MAINVIEW for OS/390 or both? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.*tableid*.OD Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Default - Any Table Actions	Can the user enter a view action for the current CMF MONITOR or MAINVIEW for OS/390 view? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMVS.*targetid*.*tableid*.AO Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Default - Primary Actions (All Views)	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the CSMON or SYSPROG command in the current MAINVIEW for OS/390? This default resource controls the following specific primary actions: • MVMVS Primary Action - CSMON • MVMVS Primary Action - SYSPROG Enabling, disabling, or changing this resource automatically enables, disables, or changes both the CSMON and SYSPROG utilities. These utilities can be enabled, disabled, or changed on an individual basis. **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.CSMON.PA BBM.MVMVS.*targetid*.SYSPROG.PA **Note:** SYSPROG services can be accessed through MAINVIEW for OS/390 and through TSO as line commands. They can also be executed as a batch job or started task. To secure these services absolutely, you ***must*** secure SYSPROG through the BBSEC member of SYS1.PARMLIB or designated data set. See Chapter 8, "Securing SYSPROG and CSMON Services" on page 99 for information on securing individual services. See the *MAINVIEW for OS/390 Customization Guide* for more information.

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
Default - Specific Table Action	Can the user enter specific view actions in specific CMF MONITOR and/or MAINVIEW for OS/390 views? **Note:** If you change this resource using the SERDEF view in CMF MONITOR, the resources starting with MVMVS are changed as well. There is no effect on CMF MONITOR for the MAINVIEW for OS/390 resources, since the associated views do not display in CMF MONITOR. However, if MAINVIEW for OS/390 is installed in the same SMP zone or in a shared DASD environment, both products use the same security parameter library. Changing this resource in CMF MONITOR does impact MAINVIEW for OS/390. This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name: **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.*tableid*.*actionid*.OA Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Any Action (MVMVS or CMF Views)	Can the user enter a view action? **Default Entity Name:** BBM.MVMVS.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.AA
Addr Space - Table Data	Can the user access address space data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC201.OD
Addr Space across interval - Table Data	Can the user access address space interval data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC301.OD
Addr Space Device Use/Delay - Table Data	Can the user access address space device use/delay data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC193.OD
Addr Space Enq Use/Delay - Table Data	Can the user access address space enqueue use/delay data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC293.OD
Address Space HSM Use/Delay - Table Data	Can the user access address space HSM use/delay data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD BBM.MVMVS.*targetid*.DC393.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
Address Space JES Use/Delay - Table Data	Can the user access address space JES use/delay data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC493.OD
Address Space MSG Use/Delay - Table Data	Can the user access address space MSG use/delay data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC593.OD
Addr Space in Workload - Table Data	Can the user access address space in workload data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC101.OD
Address Space XCF Use/Delay - Table Data	Can the user access address space XCF use/delay data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC793.OD
Channel Path - Table Data	Can the user access channel path data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC124.OD
Channel Path on LCU - Table Data	Can the user access channel path on LCU data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC224.OD
Common Storage - Table Data	Can the user access common storage data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE39.OD
Coupling Facility - Table Data	Can the user access coupling facility data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE20.OD
CMF Reserve - Table Data	Can the user access CMF reserve data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE0C.OD
CMF System Interval - Table Data	Can the user access CMF system interval data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC108.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
CMF XDS API CX10XDQY/ CX10XDRC Actions	**Note:** Affects only CMF MONITOR. Can the user access a cross-system SMF buffer? **Class Name:** FACILITY **Default Entity Name:** ERBSDS.SMFDATA
CMF XDS API CX10XDGS Action	**Note:** Affects only CMF MONITOR. Can the user access cross-system type 79 performance snapshot data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.*tableid*.PA **Note:** This resource is distributed as a disabled, rather than an enabled, security call.
CPU - Table Data	Can the user access CPU data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE05.OD
Data Collect Stat - Table Data	Can the user access data for the DCSTAT view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC427.OD
Data Collect Stat - Any Action	Can the user enter a DCSTAT view action? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC427.AO
Data Collect Stat - Action - Deact	Can the user enter the D command in the DCSTAT view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC427.DEACT.OA
Data Collect Stat - Action - Activate	Can the user enter the A command in the DCSTAT view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC427.ACTIVATE.OA
DataSet I/O - Table Data	Can the user access data set I/O data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC327.OD
Device - Table Data	Can the user access device data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE22.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVScope DD Entry - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope DD views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE13.OD
Enqueue - Table Data	Can the user access enqueue data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE0B.OD
MVScope Execution Unit - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope execution unit views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE11.OD
HSM Detail Data - Table Data	Can the user access HSM detail data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE09.OD
MVScope CCW and I/O data - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope I/O CCW and data views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE2B.OD
MVScope I/O Interrupt - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope I/O interrupt views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE2A.OD
Logical Control Unit - Table Data	Can the user access logical control unit data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE23.OD
Lpar/Domain - Table Data	Can the user access LPAR/domain data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE04.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVScope Monitor Set - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope monitor set views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.OD
MVMVS Access List - Table Data	Can the user access list data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE34.OD
MVMVS Consoles - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access console data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC227.OD
MVMVS Consoles - Any Action	**Note:** Affects only MAINVIEW for OS/390. Can the user enter a view action in any MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC227.AO
MVMVS Consoles - Action - Command	**Note:** Affects only MAINVIEW for OS/390. Can the user enter an MVS command from any view of MAINVIEW for OS/390? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC227.CMD.OA
MVMVS Consoles List - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access console list data for a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC127.CMD.OD
MVMVS Primary Action - CSMON	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the CSMON command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.CSMON.PA

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVMVS DataSpace - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data space data for a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE33.OD
MVMVS Expanded Storage Info - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access expanded storage data for a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE53.OD
MVMVS Primary Action - SYSPROG	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the SYSPROG command from a MAINVIEW for OS/390 view in the current product? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.SYSPROG.PA **Note:** SYSPROG services can be accessed through MAINVIEW for OS/390, through TSO as RESOLVE commands, and in batch jobs and started tasks. To secure these services absolutely, you ***must*** secure SYSPROG through the BBSEC member of SYS1.PARMLIB. See the *MAINVIEW for OS/390 Customization Guide* for more information.
Exception Admin - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access system interval data for a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DYEM0.OD
Exception Admin - Any Action	**Note:** Affects only MAINVIEW for OS/390. Can the user enter a view action for the current MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DYEM0.AO
Exception Admin - Action - Start AEW	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Start AEW command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DYEM0.STRTAEW.OA

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
Exception Admin - Action - Stop AEW	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Stop AEW command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DYEM0.STOPAEW.OA
Exception Admin - Action - Delete Member	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Delete Member command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DYEM0.DELMEM.OA
Exception Admin - Action - Display	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Display command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVSPS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.DISPLAY.AO
Exception Admin - Action - Read Directory	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Read Directory command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVSPS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.READDIR.AO
Exception Admin - Action - Read Member	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Read Member command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVSPS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.READMEM.AO
Exception Admin - Action - Write Member	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Write Member command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVSPS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.WRITEMEM.AO
Exception Admin - Action - Active Sampler	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Active AEW Sampler command from a MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVSPS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.ACTSAMPL.AO

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVMVS Warning - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access any MAINVIEW for OS/390 view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DYEM0.OD
MVMVS Wkld List - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access the WKLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC627.OD
MVMVS Wkld List - Any Action	**Note:** Affects only MAINVIEW for OS/390. Can the user enter any command from the WKLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC627.AO
MVMVS Wkld List - Action - Update	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Update command from the WKLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC627.UPDTWKLD.OA
MVMVS Wkld List - Action - Save	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the SAVE command from the WKLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC627.SAVEWKLD.OA
MVMVS Wkld List - Action - Delete	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Delete command from the WKLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC627.DLETWKLD.OA
MVMVS Wkld List - Action - Alt/Rename	**Note:** Affects only MAINVIEW for OS/390. Can the user enter the Alt/Rename command from the WKLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC627.ALTRWKLD.OA

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVScope Messages - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope explanatory texts views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC727.OD
MVScope - Action - STOp a Monitor Set	**Note:** Affects only MAINVIEW for OS/390. Can the user stop a monitor set with the STO line command from the MSLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.STOP.OA
MVMVS MVScope provide I/O data	**Note:** Affects only MAINVIEW for OS/390. Can the user start a monitor set that provides I/O data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.MVSCPDAT.PA
MVMVS Primary Action - MVSCOPE	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the MVSCOPE primary command? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.MVSCOPE.PA
MVScope - Action - MONitor start	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the MON line command from the MSLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.MONITOR.OA
MVScope - Action - M command Dxre	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command on device views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE22.MLCMD.OA
MVScope - Action - M command Asiw	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from address space in wait views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC101.MLCMD.OA

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVScope - Action - M command Wusr	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC193.MLCMD.OA
MVScope - Action - M command Asre	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from job views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC201.MLCMD.OA
MVScope - Action - M command WusrENQ	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user ENQ views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC293.MLCMD.OA
MVScope - Action - M command WusrHSM	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user HSM views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC393.MLCMD.OA
MVScope - Action - M command WusrJES	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user JES views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC493.MLCMD.OA
MVScope - Action - M command WusrMSG	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user MSG views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC593.MLCMD.OA

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVScope - Action - M command WusrWkld	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user workload views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC693.MLCMD.OA
MVScope - Action - M command WusrXCF	**Note:** Affects only MAINVIEW for OS/390. Can the user start an MVScope monitor set with the M line command from wait user XCF views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC793.MLCMD.OA
MVScope - Action - DELete a Monitor Set	**Note:** Affects only MAINVIEW for OS/390. Can the user stop a monitor set with the DEL line command from the MSLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.DELETE.OA
MVScope - Action - CHAnge a Monitor Set	**Note:** Affects only MAINVIEW for OS/390. Can the user change a monitor set with the CHA line command from the MSLIST view? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.CHANGE.OA
MVScope - Action - ADD MS line command	**Note:** Affects only MAINVIEW for OS/390. Can the user add a monitor set with the ADD line command? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.ADDLC.OA
MVScope - Action - ADD a Monitor Set	**Note:** Affects only MAINVIEW for OS/390. Can the user add a monitor set with the ADD line command? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE15.ADD.OA
MVScope Named Program Virt Stor - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope-named program virtual storage views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC512.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
Page Dataset - Table Data	Can the user access page data set data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE06.OD
MVScope Program Virt Stor - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope program virtual storage views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC412.OD
MVScope PSW Sample - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope PSW sample views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE14.OD
Summary - Table Data	Can the user access summary data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE38.OD
Swap Dataset - Table Data	Can the user access swap data set data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE07.OD
System CPU - Table Data	Can the user access system CPU data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE35.OD
System Paging - Table Data	Can the user access system paging data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE36.OD
System Swap - Table Data	Can the user access system swap data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE37.OD
SMS Storage Group - Table Data	Can the user access SMS storage group data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE03.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
SPDataSpace - View - Contents	Can the user view data from data spaces? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DD100.OD
SPDataSpace - Any Action	Can the user enter any action from data space views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMVS.*targetid*.D1000.AO
SPDataSpace - Action - Change Offset	Can the user change offset of contents being displayed in data space views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DD100.OFFSET.OA
SPDataSpace - Action - Zap Contents	Can the user alter storage from data space views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DD100.CONTENTS.OA
SPDataSpace - Action - Cancel Changes	Can the user cancel changes made to contents of data space views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DD100.CANCEL.OA
SRM Domain - Table Data	Can the user access SRM domain data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE29.OD
MVScope Time Buckets - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope time bucket views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE1E.OD
MVScope Time 8 Buckets - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope time 8 bucket views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE1F.OD
MVScope Virtual Storage - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope virtual storage views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DC112.OD

Table 15. Resource Definitions for CMF MONITOR and MAINVIEW for OS/390 (Continued)

Description of resource in SERDEF view	Resource name
MVScope Volume Extent - Table Data	**Note:** Affects only MAINVIEW for OS/390. Can the user access data for MVScope volume extent views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE2C.OD
Workload - Table Data	Can the user access workload data? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE0E.OD
Workload - WLM Ext Period - Table Data	**Note:** Affects only CMF MONITOR (5.2.3 and later) and MAINVIEW for OS/390 (2.4.2 and later). Can the user access workload data for WLM Extend Period views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE47.OD
Workload - WLM period - Table Data	**Note:** Affects only CMF MONITOR (5.2.3 and later) and MAINVIEW for OS/390 (2.4.2 and later). Can the user access workload data for WLM period views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE43.OD
Workload - WLM Server - Table Data	Can the user access workload data for WLM server views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE44.OD
Workload - WLM Subsystem - Table Data	Can the user access workload data for WLM subsystem views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE45.OD
XCF Member - Table Data	Can the user access data for XCF Member views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE52.OD
XCF Path - Table Data	Can the user access data for XCF Path views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE50.OD
XCF System - Table Data	Can the user access data for XCF System views? **Default Entity Name:** BBM.MVMVS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMVS.*targetid*.DCE51.OD

MAINVIEW Alarm Manager Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW Alarm Manager security resource:

- Display the SERDEFL view in MAINVIEW Alarm Manager, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
- Select the member you want to change that has a **Product** field of `MVALARM`.

A total of five unique entity names control all MAINVIEW Alarm Manager resources. To enable or disable all security for MAINVIEW Alarm Manager, you need only disable or enable the following high-level resources.

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Action
- Any Action (MVALARM Views)

The following table lists all resources that are protected by MAINVIEW Alarm Manager. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any subsituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is automatically transformed to external resource class `FACILITY`.

Table 16. Resource Definitions for MAINVIEW Alarm Manager

Description of resource in SERDEF view	Resource name
Default - Table Data	Can the user access a MAINVIEW Alarm Manager View? This default resource controls a subset of similar resources. Enabling, disabling or changing this resource automatically enables, disables, or changes all resources with the following default entity name. Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVALARM.*targetid*.@DFLT.OD
Default - Any Table Actions	Can the user enter a view action for the current MAINVIEW Alarm Manager view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVALARM.*targetid.tableid.*AO
Default - Alter Data Set	Can the user access a MAINVIEW Alarm Manager data set? **Class Name:** DATASET **Entity Name:** &DSN

Table 16. Resource Definitions for MAINVIEW Alarm Manager (Continued)

Description of resource in SERDEF view	Resource name
Default - Specific Table Action	Can the user enter specific view commands from MAINVIEW Alarm Manager views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.*tableid*. *actionid*.OA
Any Action - (MAINVIEW Alarm Manager Views)	Can the user enter a view action in the current MAINVIEW Alarm Manager product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.AA
Alarm Definitions - Alter Data Set	Can the user access a MAINVIEW Alarm Manager data set where alarm definitions reside? **Class Name:** DATASET **Entity Name:** &DSN
Alarm Groups - Table Data	Can the user access data for MAINVIEW Alarm Manager alarm group and alarm definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.OD
Alarm Groups - Action - Enable/Disable	Can the user change the runtime status of alarm groups in MAINVIEW Alarm Manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPRTSTC.OA
Alarm Groups - Action - Rename	Can the user enter the R (RENAME) line command in the ALGLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPRNM.OA
Alarm Groups - Action - Install	Can the user enter the INSTall primary command in the ALGEDI01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPRINST.OA
Alarm Groups - Action - Force Delete	Can the user enter the F (FORCE) line command in the ALGLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPRFORCE.OA
Alarm Groups - Action - Delete	Can the user enter the D (DELETE) line command in the ALGLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPDEL.OA
Alarm Groups - Action - Copy	Can the user enter the C (COPY) line command in the ALGLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPCOPY.OA

Table 16. Resource Definitions for MAINVIEW Alarm Manager (Continued)

Description of resource in SERDEF view	Resource name
Alarm Groups - Action - Add	Can the user enter the A (ADD) line command in the ALGLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA20.GRPADD.OA
Alarm Groups/ Definitions - Any Action	Can the user enter actions for MAINVIEW Alarm Manager alarm group or definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA80.AO
Alarm Definitions - Table Data	Can the user access data for MAINVIEW Alarm Manager alarm group and alarm definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.OD
Alarm Definitions - Action - Save (UPD)	Can the user enter the SAVE primary command in the ALGEDI01 and ALMEDI01 views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFUPD.OA
Alarm Definitions - Action - Enable/Disable	Can the user change the runtime status of alarm definitions in MAINVIEW Alarm Manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFRTSTC.OA
Alarm Definitions - Action - Rename	Can the user enter the R (RENAME) line command in the ALMLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFRNM.OA
Alarm Definitions - Action - Install Primary Command	Can the user enter the INSTall primary command in the alarm group and alarm definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFINST.OA
Alarm Definitions - Action - Install Line Command	Can the user enter the I (INSTALL) line command in the ALMLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFINST.OA
Alarm Definitions - Action - Delete	Can the user enter the D (DELETE) line command in the ALMLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFDEL.OA
Alarm Definitions - Action - Copy	Can the user enter the C (COPY) line command in the ALMLST01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFCOPY.OA

Table 16. Resource Definitions for MAINVIEW Alarm Manager (Continued)

Description of resource in SERDEF view	Resource name
Alarm Definitions - Action - Save (ADD)	Can the user enter the SAVE primary command in the ALMADD01 view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA10.DEFADD.OA
Alarm Messages - Table Data	Can the user access data for MAINVIEW Alarm Manager alarm message views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA30.OD
Alarm Thresholds - Table Data	Can the user access data for MAINVIEW Alarm Manager alarm group and alarm definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVALARM.*targetid*.HAA80.OD

MAINVIEW for CICS Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for CICS security resource:

- Display the SERDEFL view in MAINVIEW for CICS, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
- Select the member you want to change that has a **Product** field of `MVCICS`.

A total of five unique entity names control all MAINVIEW for CICS resources. To enable or disable all security for MAINVIEW for CICS, you need only disable or enable the following high-level resources.

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Action
- Any Action (MVCICS Views)

The following table lists all resources that are protected by MAINVIEW for CICS. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any subsituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 17. Resource Definitions for MAINVIEW for CICS

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access MAINVIEW for CICS views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.*tableid*.OD
Default - Any Table Actions	Can the user enter any view commands from MAINVIEW for CICS views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVCICS.*targetid*.*tableid*.AO
Default - Alter Data Set	Can the user alter MAINVIEW for CICS data sets? **Entity Name:** &DSN
Default - Specific Table Action	Can the user enter specific view commands from MAINVIEW for CICS views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVCICS.*targetid*.*tableid*.*actionid*.OA
Any Action - (MAINVIEW for CICS Views)	Can the user enter any command from MAINVIEW for CICS views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVCICS.*targetid*.AA
Appl Monitor - Table Data	Can the user access MAINVIEW for CICS monitor table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAA1Q.OD
Workload Definitions - Table Data	Can the user access workload definition table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAB10.OD
Workload Definitions - Any Action	Can the user enter any commands from MAINVIEW for CICS workload definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAB10.AO
Workload Definitions - Action - Install	Can the user install MAINVIEW for CICS workload definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAB10.OA
Workload Definitions - Action - Edit	Can the user edit MAINVIEW for CICS workload definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAB10.*actionid*.OA
Workload Definitions - Alter Data Set	Can the user alter MAINVIEW for CICS workload definitions? **Entity Name:** &DSN

Table 17. Resource Definitions for MAINVIEW for CICS (Continued)

Description of resource in SERDEF view	**Resource name**
Application Workload - Table Data	Can the user access application workload table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAB10.OD
Monitor - Table Data	Can the user access application monitor table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KAA10.OD
CORT - Table Data	Can the user access components of response time table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KCA10.OD
REGION - Table Data	Can the user access region table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVCICS.*targetid*.KRE10.OD

MAINVIEW for DATA ACCELERATOR Compression

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for DATA ACCELERATOR Compression security resource:

- Display the SERDEFL view in MAINVIEW for DATA ACCELERATOR Compression, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
- Select the member you want to change that has a **Product** field of `MVDAC`.

A total of four unique entity names control all MAINVIEW for DATA ACCELERATOR Compression resources. To enable or disable all security for MAINVIEW for DATA ACCELERATOR Compression, you need only disable or enable the following high-level resources.

- Default - Table Data
- Default - Any Table Actions
- Default - Specific Table Action
- Any Action (MVDAC Views)

The following table lists all resources that are protected by MAINVIEW for DATA ACCELERATOR Compression. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any subsituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is automatically transformed to external resource class `FACILITY`.

Table 18. Resource Definitions for MAINVIEW for DATA ACCELERATOR Compression

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user acess a view in MAINVIEW for DATA ACCELERATOR Compression? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDAC.*targetid*.*tableid*.OD
Default - Any Table Actions	Can the user enter a view action for the current MAINVIEW for DATA ACCELERATOR Compression view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVDAC.*targetid*.*tableid*.AO
Default - Specific Table Action	Can the user enter specific view actions in specific MAINVIEW for DATA ACCELERATOR Compression views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OA **Entity Name after Substitution:** BBM.MVDAC.*targetid*.*tableid*.OA
Any Action (MVDAC Views)	Can the user enter a view action? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AA **Entity Name after Substitution:** BBM.MVDAC.*targetid*.*tableid*.AA

Table 18. Resource Definitions for MAINVIEW for DATA ACCELERATOR Compression (Continued)

Description of resource in SERDEF view	Resource name
DAC Statistics - Table Data	Can the user view the DAC Statistics? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDAC.*targetid*.DC200.OD
DAC Regiset Statistics - Table Data	Can the user view the DAC Register Statistics? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDAC.*targetid*.DC500.OD
DAC SMS Statistics - Table Data	Can the user view the DAC SMS Statistics? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDAC.*targetid*.DC600.OD
MVS Catalog - Table Data	Can the user view the MVS Catalog? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDAC.*targetid*.DC300.OD

MAINVIEW for DB2 Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for DB2 security resource:

1. Display the SERDEFL view in MAINVIEW for DB2, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVDB2`.

A total of five unique entity names control all MAINVIEW for DB2 resources. To enable or disable all security for MAINVIEW for DB2, you need only disable or enable all of the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Actions
- Any Action (MAINVIEW for DB2 Views)

The following table lists all the security resources that are protected by MAINVIEW for DB2. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 19. Resource Definitions for MAINVIEW for DB2

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access MAINVIEW for DB2 views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid.tableid.*OD
Default - Any Table Actions	Can the user enter any view commands from MAINVIEW for DB2 views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVDB2.*targetid.tableid.*AO
Default - Alter Data Set	Can the user alter MAINVIEW for DB2 data sets? **Class Name:** DATASET **Entity Name:** &DSN
Default - Specific Table Action	Can the user enter specific view commands from MAINVIEW for DB2 views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVDB2.*targetid.tableid. actionid.*OA

Table 19. Resource Definitions for MAINVIEW for DB2 (Continued)

Description of resource in SERDEF view	Resource name
Any Action - (MAINVIEW for DB2 Views)	Can the user enter any command from MAINVIEW for DB2 views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVDB2.*targetid*.AA
Appl Monitor - Table Data	Can the user access MAINVIEW for DB2 application monitor table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAA1Q.OD
Workload Definitions - Table Data	Can the user access workload definition table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAB10.OD
Workload Definitions - Any Action	Can the user enter any commands from MAINVIEW for DB2 workload definitions? **Default Entity Name: Entity Name after Substitution:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAB10.OA
Workload Definitions - Action - Install	Can the user install MAINVIEW for DB2 workload definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAB10.*actionid*.OA
Workload Definitions - Action - Edit	Can the user edit MAINVIEW for DB2 workload definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAB10.*actionid*.OA
Workload Definitions - Alter Data Set	Can the user alter MAINVIEW for DB2 workload definitions? **Class Name:** DATASET **Entity Name:** &DSN
Application Workload - Table Data	Can the user access application workload table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAA1J.OD
Monitor - Table Data	Can the user access application monitor table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PAA10.OD
Status - Table Data	Can the user access DB2 status table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PS100.OD

Table 19. Resource Definitions for MAINVIEW for DB2 (Continued)

Description of resource in SERDEF view	**Resource name**
BufferPool - Table Data	Can the user access buffer pool table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PBF00.OD
IoActivity - Table Data	Can the user access I/O activity (page set) table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PI010.OD
LockOuts - Table Data	Can the user access lockout table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PL020.OD
Users - Table Data	Can the user access users (thread) table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PU010.OD
ZPARM - Table Data	Can the user access ZPARM table data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PZ100.OD
ZPARM - Any Table Data	Can the user enter any action in the ZPARM views to change DB2 parameters through OPERTUNE? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVDB2.*targetid*.PZ100.AO

MAINVIEW Explorer

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW Explorer security resource:

- Display the SERDEFL view in MAINVIEW Explorer, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
- Select the member you want to change that has a **Product** field of `MVEXP`.

A single unique entity name controls all MAINVIEW Explorer resources. To enable or disable all security for MAINVIEW Explorer, you need only disable or enable the following high-level resource.

- Default - Table Data

The following table lists all resources that are protected by MAINVIEW Explorer. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any subsituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is automatically transformed to external resource class `FACILITY`.

Table 20. Resource Definitions for MAINVIEW Explorer

Description of resource in SERDEF view	**Resource name**
Server Info - Table Data	Can the user view MAINVIEW Host Server information? **Default Entity Name:** BBW.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBW.MVEXP.*targetid*.WIF01.OD
Session Info - Table Data	Can the user view client session information from the MAINVIEW Host Server? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBW.MVEXP.*targetid*.WIF10.OD

MAINVIEW for IMS Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for IMS resource:

1. Display the SERDEFL view in MAINVIEW for IMS, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVIMS`.

A total of five unique entity names control all MAINVIEW for IMS resources. To enable or disable all security for MAINVIEW for IMS, you need only disable or enable the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Actions
- Any Action (MAINVIEW for IMS Views)

The following table lists all resources protected by MAINVIEW for IMS. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 21. Resource Definitions for MAINVIEW for IMS

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access a MAINVIEW for IMS view? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.@DFLT.OD Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Default - Any Table Actions	Can the user enter a view action for the current MAINVIEW for IMS view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVIMS.*targetid*.*tableid*.AO
Default - Specific Table Action	Can the user enter specific view actions from MAINVIEW for IMS views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.*tableid*.*actionid*.OA

Table 21. Resource Definitions for MAINVIEW for IMS (Continued)

Description of resource in SERDEF view	Resource name
Default - Alter Data Set	Can the user access a MAINVIEW for IMS data set? **Class Name:** DATASET **Entity Name:** &DSN
Any Action (MAINVIEW for IMS Views)	Can the user enter a view action in the current MAINVIEW for IMS product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.AA
Appl Workload - Table Data	Can the user access data for MAINVIEW for IMS application workload views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAA1J.OD
Monitor - Table Data	Can the user access data for MAINVIEW for IMS monitor views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAA10.OD
Appl Monitor - Table Data	Can the user access data for MAINVIEW for IMS application monitor views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAA1Q.OD
Workload Definitions - Table Data	Can the user access data for MAINVIEW for IMS workload definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB10.OD
Workload Definitions - Any Action	Can the user enter actions for MAINVIEW for IMS workload definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB10.AO
Workload Definitions - Action - Edit	Can the user enter the EDIT command in MAINVIEW for IMS workload definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB10.EDIT.OD
Workload Definitions - Alter Data Set	Can the user access a MAINVIEW for IMS data set where workload definitions reside? **Class Name:** DATASET **Entity Name:** &DSN
Workload Definitions - Action - Install	Can the user enter the INStall command in workload definition views of MAINVIEW for IMS? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB10.INSTALL.OA

Table 21. Resource Definitions for MAINVIEW for IMS (Continued)

Description of resource in SERDEF view	Resource name
IMS Overview - Table Data	Can the user access data for MAINVIEW for IMS overview views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPA10.OD
Region Occupancy - Table Data	Can the user access data for MAINVIEW for IMS region occupancy views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after SubstitutionEntity Name after Substitution:** BBM.MVIMS.*targetid*.FPA20.OD
Class Activity - Table Data	Can the user access data for MAINVIEW for IMS class activity views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPA30.OD
Transaction - Table Data	Can the user access data for MAINVIEW for IMS transaction views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after SubstitutionEntity Name after Substitution:** BBM.MVIMS.*targetid*.FPA40.OD
Balancing Group - Table Data	Can the user access data for MAINVIEW for IMS balancing group views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPA50.OD
Tran Sample Event - Table Data	Can the user access data for MAINVIEW for IMS transaction event views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPC10.OD
Tran I/O - Table Data	Can the user access data for MAINVIEW for IMS transaction input/output views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPC20.OD
Tran Lock - Table Data	Can the user access data for MAINVIEW for IMS transaction lock views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPC30.OD
Tran Latch - Table Data	Can the user access data for MAINVIEW for IMS transaction latch views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FPC40.OD
Trace Datasets - Table Data	Can the user access data for MAINVIEW for IMS trace data sets? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FP210.OD

Table 21. Resource Definitions for MAINVIEW for IMS (Continued)

Description of resource in SERDEF view	Resource name
Sampler Admin - Table Data	Can the user access data for MAINVIEW for IMS sampler administration views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB20.OD
Sampler Definitions - Any Action	Can the user enter a view action in the sampler definition view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB20.A0
Sampler Definitions - Action - Edit	Can the user enter the EDIT command in sampler definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB20.EDIT.OA
Sampler Definitions - Alter Data Set	Can the user access a sampler definition BBPARM data set? **Class Name:** DATASET **Entity Name**: &DSN
Sampler Definitions - Action - Install	Can the user enter the INStall command in the sampler definitions view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB20.INSTALL.OA
Sampler Operations - Table Data	Can the user access data in the sampler operations view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB30.OD
Sampler Operations - Any Action	Can the user enter an action in sampler operations view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB30.AO
Sampler Operations - Action - Start	Can the user enter the Start command in sampler operations view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB30.START.OA
Sampler Operations - Action - Stop	Can the user enter the Stop command in sampler operations view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB30.STOP.OA
Sampler Operations - Action - Quiesce	Can the user enter the Quiesce command in sampler operations view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVIMS.*targetid*.FAB30.QUIESCE.OA

MAINVIEW for IP Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for IP resource:

1. Display the SERDEFL view in MAINVIEW for IP, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVIP`.

A single entity name controls all MAINVIEW for IP resources. To enable or disable all security for MAINVIEW for IP, you need only disable or enable the following high-level resource:

- Default - Table Data

The following table lists all the resources that are protected by MAINVIEW for IP. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 22. Resource Definitions for MAINVIEW for IP

Description of resource in SERDEF view	**Resource name**
Stack(s) Information - Table Data	Can the user see Stack(s) Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP800.OD
Configuration - Table Data	Can the user see Configuration Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP810.OD
Connections - Table Data	Can the user see Connections? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP820.OD
Network Devices - Table Data	Can the user see Network Devices? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP830.OD
Ports - Table Data	Can the user see Ports? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP850.OD

Table 22. Resource Definitions for MAINVIEW for IP (Continued)

Description of resource in SERDEF view	Resource name
Routes - Table Data	Can the user see Routes? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP860.OD
Job Response - Table Data	Can the user see Job Response? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP870.OD
Port Response - Table Data	Can the user see Port Response? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP880.OD
Network Links - Table Data	Can the user see Network Links? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVIP.*targetid*.SP890.OD

MAINVIEW for MQSeries Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for MQSeries (formerly known as Command MQ for S/390) security resource:

1. Display the SERDEFL view in MAINVIEW for MQSeries, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVMQS`.

A total of five unique entity names control all MAINVIEW for MQSeries resources. To enable or disable all security for MAINVIEW for MQSeries, you need only disable or enable all of the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Actions
- Any Action (MAINVIEW for MQSeries Views)

The following table lists all the security resources that are protected by MAINVIEW for MQSeries. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 23. Resource Definitions for MAINVIEW for MQSeries

Description of resource in SERDEF view	**Resource name**
DEFAULT ENTRIES	
Default - Table Data	Can the user enter a view in MAINVIEW for MQSeries? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following default entity name: **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.*inttable*OD
Default - Any Table Actions	Can the user enter any actions against data in a view? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following default entity name: **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.@DFLT.AO
Default - Alter Data Set	Can the user alter a data set? The data set is usually a BBPARM or BBSECURE data set. This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following default entity name: **Default Entity Name:** &DATASETNAME **Entity Name after Substitution:** *datasetname*
Default - Specific Table Action	Can the user enter a specific action against data in a view? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following default entity name: **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.#DEFAULT.ACTION

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
ANY ACTION ENTRIES	
Any Action (MVMQS Views)	Can the user enter any action in MAINVIEW for MQSeries? This resource controls access to all MAINVIEW for MQSeries actions. Before you can effectively enter any action in MAINVIEW for MQSeries when this resource is enabled, this check must first be passed. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.AA
ALIAS QUEUE ENTRIES	
AliasQueue - Table Data	Can the user access MAINVIEW for MQSeries alias queue data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.OD
AliasQueue - Any Action	Can the user enter any action against MAINVIEW for MQSeries alias queues? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.AO
AliasQueue - Action - Description	Can the user alter the description of an alias queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.DESCR.OA
AliasQueue - Action - Target Queue	Can the user enter an action against a Target Alias Queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.TARGQ.OA
AliasQueue - Action - Inhibit Puts	Can the user inhibit puts against an alias queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.PUT.OA
AliasQueue - Action - Inhibit Gets	Can the user inhibit gets against an alias queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.GET.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
AliasQueue - Action - Default Message Priority	Can the user alter a default message priority? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.DEFPRTY.OA
AliasQueue - Action - Default Message Persistence	Can the user alter the default message persistence? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.DEFPSIST.OA
AliasQueue - Action - Queue Scope	Can the user alter the queue scope? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.SCOPE.OA
AliasQueue - Action - Add an AliasQueue	Can the user add an alias queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.ADD.OA
AliasQueue - Action - Delete an AliasQueue Nopurge	Can the user delete an alias queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.DELETE.OA
AliasQueue - Action - Delete an AliasQueue Purge	Can the user delete an alias queue purge? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD40.DELETEP.OA
CHANNEL ENTRIES	
Channel - Table Data	Can the user access MAINVIEW for MQSeries channel data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.OD
Channel - Any Action	Can the user enter any action against MAINVIEW for MQSeries channels? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.AO

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Channel - Action - Start	Can the user enter a start action for a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.START.OA
Channel - Action - Stop	Can the user enter a stop action for a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.STOP.OA
Channel - Action - Add	Can the user add a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.ADD.OA
Channel - Action - Delete a Channel	Can the user delete a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.DELETE.OA
Channel - Action - Reset Sequence Number	Can the user reset the sequence number for a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.RESETSEQ.OA
Channel - Action - Change Batchsize	Can the user change the batch size for a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.BATCHSZ.OA
Channel - Action - Change CONNAME	Can the user change the connection name for a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.CONNAME.OA
Channel - Action - Change Msg Conversion	Can the user change the message conversion for a channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.CONVERT.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Channel - Action - Change Channel Description	Can the user change a channel description? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.DESCR.OA
Channel - Action - Change Channel DISCINT	Can the user change the channel disconnect interval? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.DISCINT.OA
Channel - Action - Change Channel LONGRTY	Can the user change the LONGRTY value for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.LONGRTY.OA
Channel - Action - Change Channel LONGTMR	Can the user change the LONGTMR value for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTIONOA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.LONGTMR.OA
Channel - Action - Change Channel MAXMSGL	Can the user change the channel maximum message length? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MAXMSGL.OA
Channel - Action - Change Channel MCANAME	Can the user change the Message Channel Agent name? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MCANAME.OA
Channel - Action - Change Channel MCATYPE	Can the user change the Message Channel Agent type? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MCATYPE.OA
Channel - Action - Change Channel MCAUSER	Can the user change the Message Channel Agent user ID? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MCAUSER.OA
Channel - Action - Change Channel MODENAME	Can the user change the channel modename? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MODENAME.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Channel - Action - Change Channel MRDATA	Can the user change the message retry exit user data for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MRDATA.OA
Channel - Action - Change Channel MREXIT	Can the user change the message retry exit for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MREXIT.OA
Channel - Action - Change Channel MRRTY	Can the user change the message retry value for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MRRTY.OA
Channel - Action - Change Channel MRTMR	Can the user change the MRTMR value for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MRTMR.OA
Channel - Action - Change Channel MSGDATA	Can the user change the message user data for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MSGDATA.OA
Channel - Action - Change Channel MSGEXIT	Can the user change the message exit for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.MSGEXIT.OA
Channel - Action - Change Channel PASSWORD	Can the user change the password for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.PASSWORD.OA
Channel - Action - Change Channel PUTAUT	Can the user change the put authority for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.PUTAUT.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Channel - Action - Change Channel QMNAME	Can the user change the queue manager name associated with the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.QMNAME.OA
Channel - Action - Change Channel RCVDATA	Can the user change the receive exit user data for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.RCVDATA.OA
Channel - Action - Change Channel RCVEXIT	Can the user change the receive exit name for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.RCVEXIT.OA
Channel - Action - Change Channel SCYDATA	Can the user change the security exit user data for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SCYDATA.OA
Channel - Action - Change Channel SCYEXIT	Can the user change the security exit name for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SCYEXIT.OA
Channel - Action - Change Channel SENDDATA	Can the user change the send exit user data for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SENDDATA.OA
Channel - Action - Change Channel SENDEXIT	Can the user change the send exit name for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SENDEXIT.OA
Channel - Action - Change Channel SEQWRAP	Can the user change the sequence wrap for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SEQWRAP.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Channel - Action - Change Channel SHORTRTY	Can the user change the value for short retries for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SHORTRTY.OA
Channel - Action - Change Channel SHORTTMR	Can the user change the SHORTTMR value for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.SHORTTMR.OA
Channel - Action - Change Channel TPNAME	Can the user change the TP name for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.TPNAME.OA
Channel - Action - Change Channel TRPTYPE	Can the user change the transport type for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.TRPTYPE.OA
Channel - Action - Change Channel USERID	Can the user change the user ID for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.USERID.OA
Channel - Action - Change Channel XMITQ	Can the user change the transmit queue for the channel? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAC10.XMITQ.OA
CICS CHANNEL ENTRIES	
CICSChnl - Table Data	Can the user access MAINVIEW for MQSeries CICS channel data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD50.OD
MESSAGE ENTRIES	
Message - Table Data	Can the user access MAINVIEW for MQSeries message header information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAE10.OD

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Message - Any Action	Can the user enter any action against MAINVIEW for MQSeries channels? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAE10.AO
Message - Action - Delete	Can the user delete a message? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAE10.DELETE.OA
Message - Action - Requeue	Can the user enter the requeue action for a message? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAE10.REQUEUE.OA
Message - Action - Queue	Can the user enter the queue action for a message? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAE10.QUEUE.OA
Message - Message Text	Can the user access message data for a specific queue? **Default Entity Name:** &CONTEXT.#qname **Entity Name after Substitution:** *contextid*.queue.name where queue.name represents the name by which the queue is known to MAINVIEW for MQSeries
MODEL QUEUE ENTRIES	
ModelQueue - Table Data	Can the user access MAINVIEW for MQSeries model queue data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.OD
ModelQueue - Any Action	Can the user enter any action against MAINVIEW for MQSeries model queues? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.AO
ModelQueue - Action - Max Depth	Can the user change the maximum depth for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.MAXDEPTH.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
ModelQueue - Action - Low Queue Depth	Can the user alter the low queue depth indicator for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QDEPTHLO.OA
ModelQueue - Action - High Queue Depth	Can the user alter the high queue depth indicator for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QDEPTHHI,OA
ModelQueue - Action - Service Interval Threshold	Can the user change the service interval threshold for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QSVCINT.OA
ModelQueue - Action - Low Q Depth Event	Can the user change the value for a low queue depth event, for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QDPLOEV.OA
ModelQueue - Action - High Q Depth Event	Can the user change the value for a high queue depth event, for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QDPHIEV.OA
ModelQueue - Action - Max Q Depth Event	Can the user change the value for a maximum queue depth event, for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QDPMAXEV.OA
ModelQueue - Action - Service Interval Event	Can the user alter the value for a service interval event for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.QSVCIEV.OA
ModelQueue - Action - Inhibit Puts	Can the user alter the inhibit puts value for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.PUT.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
ModelQueue - Action - Inhibit Gets	Can the user alter the inhibit gets value for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.GET.OA
ModelQueue - Action - Default Message Priority	Can the user alter the default message priority for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.DEFPRTY.OA
ModelQueue - Action - Default Message Persistence	Can the user alter the default message persistence for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.DEFPSIST.OA
ModelQueue - Action - Default Open for Input	Can the user change the default open for input for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.DEFSOPT.OA
ModelQueue - Action - Shareable Option	Can the user change the shareable option for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.SHARE.OA
ModelQueue - Action - Message Delivery Sequence	Can the user alter the message delivery sequence for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.MSGDLVSQ.OA
ModelQueue - Action - Storage Class	Can the user change the storage class for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.STGCLASS.OA
ModelQueue - Action - Max Message Length	Can the user change the maximum message length? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.MAXMSGL.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
ModelQueue - Action - Description	Can the user change the description of a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.DESCR.OA
ModelQueue - Action - Process Name	Can the user change the process name for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.PROCESS.OA
ModelQueue - Action - Retention Interval	Can the user change the retention interval for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.RETINTVL.OA
ModelQueue - Action - Trigger Control	Can the user alter the value for trigger control for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.TRIGGER.OA
ModelQueue - Action - Trigger Type	Can the user change the trigger type for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.TRIGTYPE.OA
ModelQueue - Action - Trigger Msg Priority	Can the user change the trigger message priority for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.TRIGMPRI.OA
ModelQueue - Action - Trigger Depth	Can the user change the trigger depth for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.TRIGDPTH.OA
ModelQueue - Action - Initiation Queue	Can the user change the initiation queue associated with a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.INITQ.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
ModelQueue - Action - Trigger Data	Can the user change the value for trigger data for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.TRIGDATA.OA
ModelQueue - Action - Backout Threshold	Can the user change the backout threshold for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.BOTHRESH.OA
ModelQueue - Action - Backout Queue Name	Can the user change the name of the backout queue associated with a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.BOQNAME.OA
ModelQueue - Action - Harden Backout Get Count	Can the user change the harden backout get count for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.HARDENBO.OA
ModelQueue - Action - Queue Usage	Can the user change the value for queue usage for a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.USAGE.OA
ModelQueue - Action - Add a ModelQueue	Can the user add a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.ADD.OA
ModelQueue - Action - Delete a Queue Nopurge	Can the user delete a model queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD60.DELETE.OA
PROCESS ENTRIES	
Processes - Table Data	Can the user access MAINVIEW for MQSeries process data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.OD

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Processes - Any Action	Can the user enter any action against a MAINVIEW for MQSeries process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.AO
Processes - Action - Appl Type	Can the user change the application type for a process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.CHAPLTYP.OA
Processes - Action - Application Id	Can the user change the application ID for a process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.CHAPPLID.OA
Processes - Action - Description	Can the user change the description of a process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.CHDESC.OA
Processes - Action - Env Data	Can the user alter the environment data for a process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.CHENVIR.OA
Processes - Action - Add a Process	Can the user add a process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.ADD.OA
Processes - Action - Delete a Process	Can the user delete a process? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF30.DELETE.OA
QUEUE ENTRIES	
Queue - Table Data	Can the user access MAINVIEW for MQSeries queue data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.OD
Queue - Any Action	Can the user enter any action against MAINVIEW for MQSeries queues? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.AO

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Queue - Action - Trigger Control	Can the user change the trigger control value for the queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.TRIGGER.OA
Queue - Action - Trigger Type	Can the user change the trigger type for the queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.TRIGTYPE.OA
Queue - Action - Trigger Msg Priority	Can the user change the default trigger message priority for the queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.TRIGMPRI.OA
Queue - Action - Trigger Depth	Can the user change the trigger depth for the queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.TRIGDPTH.OA
Queue - Action - Trigger Data	Can the user alter the trigger data value for the queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.TRIGDATA.OA
Queue - Action - Queue Scope	Can the user change the queue scope? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.SCOPE.OA
Queue - Action - Queue Usage	Can the user alter the value for queue usage? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.USAGE.OA
Queue - Action - Add a Queue	Can the user add a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.ADD.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Queue - Action - Storage Class	Can the user alter the storage class for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.STGCLASS.OA
Queue - Action - Shareable Option	Can the user alter the shareable option for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.SHARE.OA
Queue - Action - Retention Interval	Can the user alter the retention period for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.RETINTVL.OA
Queue - Action - Service Interval Threshold	Can the user alter the service interval threshold for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QSVCINT.OA
Queue - Action - Service Interval Event	Can the user alter the service interval event value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QSVCIEV.OA
Queue - Action - Max Q Depth Event	Can the user alter the maximum queue depth event value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QDPMAXEV.OA
Queue - Action - Low Q Depth Event	Can the user alter the low queue depth event value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QDPLOEV.OA
Queue - Action - High Q Depth Event	Can the user alter the high queue depth event value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QDPHIEV.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Queue - Action - Low Queue Depth	Can the user alter the low queue depth value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QDEPTHLO.OA
Queue - Action - High Queue Depth	Can the user alter the high queue depth event value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.QDEPTHHI.OA
Queue - Action - Inhibit Puts	Can the user alter the inhibit puts value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.PUT.OA
Queue - Action - Process Name	Can the user alter the process name associated with a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.PROCESS.OA
Queue - Action - Message Delivery Sequence	Can the user alter the message delivery sequence for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.MSGDLVSQ.OA
Queue - Action - Max Message Length	Can the user alter the maximum message length for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.MAXMSGL.OA
Queue - Action - Max Depth	Can the user alter the maximum depth for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.MAXDEPTH.OA
Queue - Action - Initiation Queue	Can the user alter the initiation queue associated with a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.INITQ.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Queue - Action - Harden Backout Get Count	Can the user alter the harden backout attribute of a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.HARDENBO.OA
Queue - Action - Inhibit Gets	Can the user alter the inhibit gets value for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.GET.OA
Queue - Action - Description	Can the user alter the description associated with a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.DESCR.OA
Queue - Action - Delete a Queue Purge	Can the user enter the delete purge action against a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.DELETE.OA
Queue - Action - Delete a Queue Nopurge	Can the user enter the delete without purge action against a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA BBM.MVMQS.*targetid*.SAD10.DELETEP.OA
Queue - Action - Default Open for Input	Can the user alter the default open for input attribute of a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA BBM.MVMQS.*targetid*.SAD10.DEFSOPT.OA
Queue - Action - Default Message Persistence	Can the user alter the default message persistence attribute of a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.DEFPSIST.OA
Queue - Action - Default Message Priority	Can the user alter the default message priority for a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.DEFPRTY.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Queue - Action - Backout Threshold	Can the user alter the backout threshold attribute of a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.BOTHRESH.OA
Queue - Action - Backout Queue Name	Can the user alter the backout queue name associated with a queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD10.BOQNAME.OA
QUEUE LIST ENTRIES	
Queue List - Table Data	Can the user access MAINVIEW for MQSeries queue list data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD70.OD
QUEUE MANAGER ENTRIES	
Queue Manager - Table Data	Can the user access MAINVIEW for MQSeries queue manager data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.od **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.OD
Queue Manager - Any Action	Can the user enter any action against MAINVIEW for MQSeries queue managers? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.AO
Queue Manager - Action - Trigger Interval	Can the user alter the queue manager trigger interval? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.TRIGINT.OD
Queue Manager - Action - Start/Stop Event	Can the user alter the start/stop event value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.STRSTPEV.OD
Queue Manager - Action - Remote Event	Can the user alter the remote events value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.REMOTEEV.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
Queue Manager - Action - Performance Event	Can the user alter the performance events value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.PERFMEV.OA
Queue Manager - Action - Max SyncPt Message	Can the user alter the maximum sync point value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.MAXSMSGS.OA
Queue Manager - Action - Max Handles	Can the user alter the maxium handles value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.MAXHANDS.OA
Queue Manager - Action - Local Event	Can the user alter the local events value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.LOCALEV.OA
Queue Manager - Action - Inhibit Event	Can the user alter the inhibit event value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.INHIBTEV.OA
Queue Manager - Action - Description	Can the user alter the queue manager description? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.&MVMQS.*targetid*.SAA10.DESCR.OA
Queue Manager - Action - Dead Letter Queue	Can the user alter the dead letter queue name associated with a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.DEADQ.OA
QueueManager - Action - Authority Event	Can the user alter the Authority event value for a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.AUTHOREV.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
QueueManager - Action - Default Transmission Queue	Can the user change the default transmission queue associated with a queue manager? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA10.DEFXMITQ.OA
QUEUE MANAGER DEFINITION ENTRIES	
QMgrDef - Table Data	Can the user access MAINVIEW for MQSeries queue manager definition data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD20.OD
QMgrDef - Any Action	Can the user enter any action against MAINVIEW for MQSeries queue manger definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD20.AO
QMgrDef - Action - Edit	Can the user edit queue manager definitions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD20.EDIT.OA
QMgrDef - Alter Data Set	Can the user change authorization for altering the queue manager definition data set? **Default Entity Name:** &DATASETNAME **Entity Name after Substitution:** BBIPARM.*datasetname*
REMOTE QUEUE ENTRIES	
RemoteQueue - Table Data	Can the user access MAINVIEW for MQSeries remote queue data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.OD
RemoteQueue - Any Action	Can the user enter any action against MAINVIEW for MQSeries remote queues? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.AO
RemoteQueue - Action - Description	Can the user change the description for a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.DESCR.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
RemoteQueue - Action - Transmission Queue	Can the user change the transmission queue associated with a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.XMITQ.OA
RemoteQueue - Action - Inhibit Puts	Can the user change the inhibit puts value for a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.PUT.OA
RemoteQueue - Action - Default Message Priority	Can the user change the default message priority for a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.DEFPRTY.OA
RemoteQueue - Action - Default Message Persistence	Can the user change the default message persistence for a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.DEFPSIST.OA
RemoteQueue - Action - Queue Scope	Can the user change the value of the queue scope for a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.SCOPE.OA
RemoteQueue - Action - Remote Qmgr Name	Can the user change the remote queue manager name associated with a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.RQMNAME.OA
RemoteQueue - Action - Remote Queue Name	Can the user change a remote queue name? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.RNAME.OA
RemoteQueue - Action - Add a RemoteQueue	Can the user add a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.ADD.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
RemoteQueue - Action - Delete a RemoteQueue Nopurge	Can the user delete a remote queue? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.DELETE.OA
RemoteQueue - Action - Delete a RemoteQueue Purge	Can the user delete a remote queue purge? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAD30.DELETEP.OA
TOPOLOGY ENTRIES	
Topology - Table Data	Can the user access MAINVIEW for MQSeries topology data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA20.OD
BUFPOOL ENTRY	
BufPool - Table Data	Can the user access Buffer Pool views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA40.OD
PAGESET ENTRY	
PageSet - Table Data	Can the user access PageSet views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAA60.OD
STORAGE CLASS ENTRIES	
StorageClass- Table Data	Can the user access StorageClass views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.OD
StorageClass- Any Action	Can the user enter any action against storage classes in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.AO
StorageClass- Action - Change XCF Group	Can the user change storage classes in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.STCXCF.OA

Table 23. Resource Definitions for MAINVIEW for MQSeries (Continued)

Description of resource in SERDEF view	Resource name
StorageClass-Action - Change PagaeSet	Can the user change the PageSet ID in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.STCPSID.OA
StorageClass-Action - Change Descript	Can the user change the storage class description in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.STCDESCR.OA
StorageClass-Action - Delete StorageC	Can the user enter the DELETE action for storage classes in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.DELETE.OA
StorageClass-Action - Add new Storage	Can the user enter the ADD action for storage classes in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF10.ADD.OA
THREAD ENTRIES	
Thread - Table Data	Can the user access thread views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF40.OD
Thread - Any Action	Can the user enter any actions against threads in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF40.AO
Thread - Action - Resolve InDoubt	Can the user enter the RESOLVE action against threads in MAINVIEW for MQSeries? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVMQS.*targetid*.SAF40.RESOLVE.OA

MAINVIEW SYSPROG Services Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW SYSPROG Services security resource:

- Display the SERDEFL view in MAINVIEW SYSPROG Services, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
- Select the member you want to change that has a **Product** field of `MVSPS` or `MVCSMON`.

Note: MAINVIEW SYSPROG Services implements two separate service points: MVSPS and MVCSMON. The resource entity name that protects the CSMON primary action depends on which service point the window is connected to when the action is issued.

A total of five unique entity names control all MAINVIEW SYSPROG Services resources from the MVSPS service point. To enable or disable all security for the MVSPS service point, you need only disable or enable the following high-level resources.

- Default - Table Data
- Default - Any Table Actions
- Default - Primary Actions (All Views)
- Default - Specific Table Action
- Any Action (MVSPS Views)

One additional entity name controls resources from the MVCSMON service point. To enable or disable all security for the MVCSMON service point, you need only disable or enable the following high-level resource.

- Default - Primary Actions (All Views)

Table 24 on page 252 lists all resources that are protected by the MVSPS service point. Table 25 on page 254 lists the resources that are protected by the MVCSMON service point. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any subsituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is automatically transformed to external resource class `FACILITY`.

Table 24. Resource Definitions for MAINVIEW SYSPROG Services - MVSPS Service Point

Description of resource in SERDEF view	Resource name
Default - Table Data	Can the user acess a view in MAINVIEW SYSPROG Services? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVSPS.*targetid*.*tableid*.OD
Default - Any Table Actions	Can the user enter a view action for the current MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.*tableid*.AO
Default - Primary Actions (All Views)	Can the user enter the CSMON or SYSPROG command in the current MAINVIEW SYSPROG Services? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.PA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.*tableid*.PA
Default - Specific Table Action	Can the user enter specific view actions in specific MAINVIEW SYSPROG Services views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.*tableid*.OA
Any Action (MVSPS Views)	Can the user enter a view action? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.*tableid*.AA
MVSPS Primary Action - CSMON	Can the user enter the CSMON command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.CSMON.PA
MVSPS Primary Action - SYSPROG	Can the user enter the SYSPROG command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.SYSPROG.PA
Consoles List - Table Data	Can the user access console list data for a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DC127.OD
Console Service - Table Data	Can the user access console service data for a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DC227.OD
Console Service - Any Action	Can the user enter any action for console service data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DC227.AO

Table 24. Resource Definitions for MAINVIEW SYSPROG Services - MVSPS Service Point (Continued)

Description of resource in SERDEF view	Resource name
Console Service - Action - Command	Can the user enter a specific command for console service data? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DC227.CMD.OA
Exception Admin - Table Data	Can the user access system interval data for a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.OD
Exception Admin - Any Action	Can the user enter a view action for the current MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.AO
Exception Admin - Action - Start AEW	Can the user enter the Start AEW command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.STRTAEW.OA
Exception Admin - Action - Stop AEW	Can the user enter the Stop AEW command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.STOPAEW.OA
Exception Admin - Action - Delete Member	Can the user enter the Delete Member command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.DELMEM.OA
Exception Admin - Action - Display	Can the user enter the Display command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.DISPLAY.OA
Exception Admin - Action - Read Directory	Can the user enter the Read Directory command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.READDIR.OA
Exception Admin - Action - Read Member	Can the user enter the Read Member command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.READMEM.OA

Table 24. Resource Definitions for MAINVIEW SYSPROG Services - MVSPS Service Point (Continued)

Description of resource in SERDEF view	Resource name
Exception Admin - Action - Write Member	Can the user enter the Write Member command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.WRITEMEM.OA
Exception Admin - Action - Active Sampler	Can the user enter the Active AEW Sampler command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.ACTSAMPL.OA
Warning - Table Data	Can the user access any MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVSPS.*targetid*.DYEM0.OD

Table 25. Resource Definitions for MAINVIEW SYSPROG Services - MVCSMON Service Point

Description of resource in SERDEF view	Resource name
Default - Primary Actions (All Views)	Can the user enter the CSMON command in the current MAINVIEW SYSPROG Services? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.PA **Entity Name after Substitution:** BBM.MVCSMON.*targetid*.*tableid*.PA
MVCSMON Primary Action - CSMON	Can the user enter the CSMON command from a MAINVIEW SYSPROG Services view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVCSMON.*targetid*.CSMON.PA

MAINVIEW for UNIX System Services Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for UNIX System Services resource:

1. Display the SERDEFL view in MAINVIEW for UNIX System Services, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVUSS`.

A total of five unique entity names control all MAINVIEW for UNIX System Services resources. To enable or disable all security for MAINVIEW for UNIX System Services, you need only disable or enable all of the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Primary Actions (All Views)
- Default - Specific Table Actions
- Any Action

The following table lists all the resources that are protected by MAINVIEW for UNIX System Services. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 26. Resource Definitions for MAINVIEW for UNIX System Services

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access a view in MAINVIEW for UNIX System Services? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.*tableid*.OD Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Default - Any Table Actions	Can the user enter a view action for the current MAINVIEW for UNIX System Services view? This default resource controls a subset of similar individual resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVUSS.*targetid*.*tableid*.AO Specific resources with this same default entity name can be enabled, disabled, or changed on an individual basis.
Default - Primary Actions (All Views)	Can the user enter the OEDGTRC command in the current MAINVIEW for UNIX System Services? **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTACTION.PA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.ACTION.PA
Default - Specific Table Action	Can the user enter specific view actions in specific MAINVIEW for UNIX System Services views? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.*tableid*.*actionid*.OA Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Any Action (MVUSS Views)	Can the user enter a view action? **Default Entity Name:** BBM.MVUSS.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.AA

Table 26. Resource Definitions for MAINVIEW for UNIX System Services (Continued)

Description of resource in SERDEF view	Resource name
Data Collect Stat - Table Data	Can the user access data for the DCSTAT view? **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UC427.OD
Data Collect Stat - Any Action	Can the user enter a DCSTAT view action? **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UC427.AO
Data Collect Stat - Action - Deact	Can the user enter the D command in the DCSTAT view? **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UC427.DEACT.OA
Data Collect Stat - Action - Activate	Can the user enter the A command in the DCSTAT view? **Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UC427.ACTIVATE.OA
Filesys/mountparm - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCED1.OD
Filesys/mountpoint - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCED0.OD
Filesystems Mounted - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC2.OD
File Space Usage - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC3.OD
HFS Global Buffers - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCED4.OD
HFS Filesystem - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCED3.OD
Global - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCED2.OD
Access All OEDG Requests	**Default Entity Name:** BBM.&PRODUCT.&CONTEXT.OEDGREQS **Entity Name after Substitution:** BBM.*productid*.*targetid*.USRQ0.OD
Process - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC0.OD
Process/command - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCECE.OD
Process/cwd - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCECF.OD

Table 26. Resource Definitions for MAINVIEW for UNIX System Services (Continued)

Description of resource in SERDEF view	Resource name
Process/path - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCECD.OD
Process/tty - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCECC .OD
Process Files Open - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCECB.OD
Process Tree - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCECA .OD
Required Processes - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCED5 .OD
Request Status - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC9.OD
Select - Action - S command Fmre	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC2.SELECT.OA
Select - Action - S command Fsre	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC3.SELECT .OA
System Parameters - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCEC4 .OD
WLM Address Space - Table Data	**Default Entity Name:** BBM.MVUSS.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVUSS.*targetid*.UCE48.OD

MAINVIEW VistaPoint Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW VistaPoint security resource:

1. Display the SERDEFL view in VistaPoint.
2. Select the member you want to change that has a **Product** field value of `MVVP`.

A total of five unique entity names control all MAINVIEW VistaPoint resources. To enable or disable all security for VistaPoint, you need only disable or enable the following high-level resources:

- Default - Table Data
- Default - Any Table Actions
- Default - Alter Data Set
- Default - Specific Table Actions
- Any Action (VistaPoint Views)

The following table lists all resources that are protected by MAINVIEW VistaPoint. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource. For a description of how the symbolics are used, see page 111.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 27. Resource Definitions for MAINVIEW VistaPoint

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access a VistaPoint view? This default resource controls a subset of similar resources. Enabling, disabling, or changing this resource automatically enables, disables, or changes all resources with the following entity name. **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVP.*targetid*.*tableid*.OD Specific resources belonging to this subset can be enabled, disabled, or changed on an individual basis.
Default - Any Table Actions	Can the user enter a view action for the current VistaPoint view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.AO **Entity Name after Substitution:** BBM.MVVP.*targetid*.*tableid*.AO
Default - Alter Data Set	Can the user access a VistaPoint data set? **Class Name:** DATASET **Entity Name:** &DSN

Table 27. Resource Definitions for MAINVIEW VistaPoint (Continued)

Description of resource in SERDEF view	Resource name
Default - Specific Table Actions	Can the user enter specific view actions from VistaPoint views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.&INTACTION.OA **Entity Name after Substitution:** BBM.MVVP.*targetid*.*tableid*.*actionid*.OA
Any Action (VistaPoint Views)	Can the user enter a view action in the current VistaPoint product? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.AA **Entity Name after Substitution:** BBM.MVVP.*targetid*.AA
Appl Definition - Table Data	Can the user access data for VistaPoint workload definition views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVP.*targetid*.JAA20.OD
Appl Workload - Table Data	Can the user access data for VistaPoint application workload views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVP.*targetid*.JAA1J.OD
Monitor - Table Data	Can the user access data for VistaPoint monitor views? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVP.*targetid*.JAA1Q.OD

MAINVIEW for VTAM Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for VTAM resource:

1. Display the SERDEFL view in MAINVIEW for VTAM, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVVTAM`.

A single entity name controls all MAINVIEW for VTAM resources. To enable or disable all security for MAINVIEW for VTAM, you need only disable or enable the following high-level resource:

- Default - Table Data

The following table lists all the resources that are protected by MAINVIEW for VTAM. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 28. Resource Definitions for MAINVIEW for VTAM

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access a MAINVIEW for VTAM view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.*tableid*.OD
Applications - Table Data	Can the user see VTAM Applications? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP100.OD
LUs - Table Data	Can the user see LUs ? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP200.OD
Transactions - Table Data	Can the user see Transactions? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP300.OD
Application Resources - Table Data	Can the user see Application Resources? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP400.OD

Table 28. Resource Definitions for MAINVIEW for VTAM (Continued)

Description of resource in SERDEF view	**Resource name**
LU Resources - Table Data	Can the user see LU Resources? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP500.OD
Transaction Resources - Table Data	Can the user see Transaction Resources? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP600.OD
Application Connections - Table Data	Can the user see Application Connections? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP700.OD
Application Availability - Table Data	Can the user see Application Availabilty? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP800.OD
3270 Statistics - Table Data	Can the user see 3270 statistics? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVVTAM.*targetid*.SP920.OD

MAINVIEW for WebSphere Resources

To disable, enable, or customize resource access authorization requests to the ESM for a MAINVIEW for WebSphere resource:

1. Display the SERDEFL view in MAINVIEW for WebSphere, as described in "Displaying a List of Members using the SERDEFL View" on page 164.
2. Select the member you want to change that has a **Product** field value of `MVWEB`.

A single entity name controls all MAINVIEW for WebSphere resources. To enable or disable all security for MAINVIEW for WebSphere, you need only disable or enable the following high-level resource:

- Default - Table Data

The following table lists all the resources that are protected by MAINVIEW for WebSphere. The **Default Entity Name** is the entity name shared by a set of similar resources and is used for high-level control of the entire set. The **Entity Name after Substitution** is the entity name with any substituted symbolic values for a particular resource.

The class name for all resources, unless otherwise indicated, is `$BBM`, which is usually, and by default, transformed to external resource class `FACILITY`.

Table 29. Resource Definitions MAINVIEW for WebSphere

Description of resource in SERDEF view	**Resource name**
Default - Table Data	Can the user access a MAINVIEW for WebSphere view? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.*tableid*.OD
Web Server Information - Table Data	Can the user see the Web Server Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP100.OD
Hourly Errors - Table Data	Can the user see the Web Server Performance Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** 'BBM.MVWEB.*targetid*.SP110.OD
Requests - Table Data	Can the user see theWeb Server Requests? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP120.OD
Responses - Table Data	Can the user see the Web Server responses? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP130.OD

Table 29. Resource Definitions MAINVIEW for WebSphere (Continued)

Description of resource in SERDEF view	**Resource name**
Cache - Table Data	Can the user see the Web Server Cache Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP140.OD
Access - Table Data	Can the user see Web Server Access Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP150.OD
Errors - Table Data	Can the user see Web Server Errors? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP160.OD
Hourly Errors - Table Data	Can the user see Web Server Hourly Access Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** 'BBM.MVWEB.*targetid*.SP170.OD'
Hourly Errors - Table Data	Can the user see Web Server Hourly Errors Information? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP180.OD
Client Response Times - Table Data	Can the user see Web Server Client Response Times? **Default Entity Name:** BBM.&PRODUCT.&CONTEXT.&INTTABLE.OD **Entity Name after Substitution:** BBM.MVWEB.*targetid*.SP200.OD

Chapter 16. Resource Definitions Listed by View

The tables in the following sections list the views for each product and the name of the resource definition, as shown in the SERDEF view, used by each view.

Common Views

Table 30 lists distributed views common to all products and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all common views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the `COMMON` security parameter member.

Table 30. Common Views

View	Resource Definition
DIAGMSG	XMsgDiagStatus - Table Data
DSLIST	Hist Data Set List - Table Data
SCREENS	ScrnTable - Table Data
SERDEF SERDEFD SERDEFE SERDEFEX SERDEFOV	ResDefDef - Table Data
SERDEFL	ResDefList - Table Data
VIEWS	ViewTable - Table Data

Plex Manager Views

Table 31 lists distributed Plex Manager views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all Plex Manager views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the `PLEXMGR` security parameter member.

Table 31. Plex Manager Views

View	Resource Definition
ADMIN	ViewTable - Table Data
CASACT	CASAction - Table Data
CASDEF CASDEFD	CASDefn - Table Data
CONACT CONACTD CONACTZ CONASEL	SSIContextMem - Table Data
CONDEF CONDEFD	SSIContext - Table Data
CONDEFL	SSIContextLst - Table Data
DIAG	ViewTable - Table Data
DIAGCONN	DiagConn - Table Data
DIAGSESS	Sessions - Table Data
DIAGSYS	Systems- Table Data
EZSEC EZSECRES	ViewTable - Table Data
MAIN	ViewTable - Table Data
OPS	ViewTable - Table Data
PLEX PLEXOVER	PlexTable - Table Data
PRODSEL	PlexTable - Table Data
SECDEF SECDEFD	SecClass - Table Data
SECDEFL	SecClassList - Table Data
SECURITY	ViewTable - Table Data
SELTAB	SelectorTable - Table Data
SEPDEF SEPDEFD	SecParms - Table Data

Table 31. Plex Manager Views

View	Resource Definition
SEPDEFL	SecParList - Table Data
SERDEFC SERDEFP	PlexTable - Table Data
TGTACT TGTACTZ TGTSEL	PlexTable - Table Data
TGTDEF TGTDEFD	TargetDef - Table Data
TGTDEFL	TargetDefLst - Table Data
USER	ViewTable - Table Data
UTILITY	ViewTable - Table Data

CMF MONITOR and MAINVIEW for OS/390 Views

Table 32 lists distributed CMF MONITOR and MAINVIEW for OS/390 views and their corresponding resource definitions. Views in **BOLD** face type require you to secure more than one resource table.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all CMF MONITOR and MAINVIEW for OS/390 views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of either CMF MONITOR or MAINVIEW for OS/390.

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views

View	Resource Definition
ARD **DDJOB** **DUJOB** **JDDEV** **JDENQ** **JHSMD** **JHSMSTAT** **JJESD** **JMSGD** **JUDEV** **JUENQ** **JXCFD** **STORC**	Addr Space - Table Data
JSUM	Addr Space across interval - Table Data
DDJOB **DUJOB** **JDDEV** **JUDEV**	Addr Space Device Use/Delay- Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
JDENQ **JUENQ**	Address Space Enq Use/Delay - Table Data
JHSMD **JHSMSTAT**	Address Space HSM Use/Delay - Table Data
JJESD	Address Space JES Use/Delay - Table Data
JMSGD	Address Space MSG Use/Delay - Table Data
ASD ASRM EZMJOB JCPU JCPUR JCPUS JDELAY JDELAYR JDELAYS JDELAYZ JFLOW JFLOWR JFLOWS JFLOWZ **JHSMD** JINFO JINFOR	Addr Space in Workload - Table Data
JPAGOVS JPAGSW JPAGSWR JPAGSWS JSRM JSRMD JSRMDR JSRMDS JSRMR JSRMS JSTOR JSTORD JSTORDR JSTORDS JSTORR JSTORS JSUM	Addr Space in Workload - Table Data
JXCFD	Address Space XCF Use/Delay - Table Data
CHANNEL	Channel Path - Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
CPSTAT **IOQ** **LCUINFO** **LCUSTAT**	Channel Path on LCU - Table Data
CSAREM CSASUM JCSA **STORC** STORCR STORCS	Common Storage - Table Data
SENQR	CMF Reserve - Table Data
EMSTAT **EXCEPT** **EZMSRM** **MPLSTAT** **SRCS** **SRMLSCT** **SRMOPT** **SYSCNFG** **SYSWKLD** **WLMMON** **WMMENU** **WMSPLX** **WMSPLXZ** **WMSYS**	CMF System Interval - Table Data
CPUINFO CPUSTAT	CPU - Table Data
DCSTAT	Data Collect Stat - Table Data
DSIO	DataSet I/O - Table Data
CDEV **DDJOB** DEV DEVINFO DEVSTAT DEVSTATZ DEVZ DSIO **DUJOB** EZMDEV **JDDEV** **JUDEV** LDEV PDEV SDEV TDEV	Device - Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
MSICCW **MSIOZ** **MSIRESP** **MSISEEK** **MSITRACE** **MSMDSN** **MSMVOL**	MVScope DD Entry - Table Data
ENQSTAT **JDENQ** **JUENQ** SENQ SENQALL SENQR	Enqueue - Table Data
MSPGM **MSTPGM** **MSTPGMZ** **MSMTASK** **MSTASK**	MVScope Execution Unit - Table Data
JHSMD **JHSMSTAT**	HSM Detail Data - Table Data
MSICCW	MVScope CCW and I/O Data - Table Data
MSICCW **MSIOZ** **MSIRESP** **MSISEEK** **MSITRACE**	MVScope I/O Interrupt - Table Data
CPSTAT **IOQ** **LCUINFO** **LCUSTAT**	Logical Control Unit - Table Data
LPARSTAT	LPAR/Domain - Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
MSDCPU MSDIAG MSDIO MSDPROF **MSICCW** **MSIOZ** **MSIRESP** **MSISEEK** **MSITRACE** MSLIST MSMAP **MSMDSN** MSMONSET **MSMTASK** **MSMVOL** **MSMVSTG** **MSPGM**	MVScope Monitor Set - Table Data
DSPCUJ	MVMVS Access List - Table Data
CONSOLE	MVMVS Consoles - Table Data
CONSOLES	MVMVS Consoles List - Table Data
DSPCINFO DSPCSTAT DSPCZ	MVMVS DataSpace - Table Data
SRMESCT	MVMVS Expanded Storage Info- Table Data
EMSTAT **EXCEPT** **EZMSRM** **MPLSTAT** **SRCS** **SRMLSCT** **SRMOPT** **SYSCNFG** **SYSWKLD** **WLMMON** **WMMENU** **WMSPLX** **WMSPLXZ** **WMSYS**	MVMVS Sys Intvl - Table Data
WARN	MVMVS Warning - Table Data
WKLIST	MVMVS Wkld List - Table Data
MSXPLAIN	MVScope Messages - Table Data
MSPGM **MSTPGM**	MVScope Named Program Virt Stor - Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
PGDINFO PGDSTAT PGSPP	Page Dataset - Table Data
MSPROG **MSPGM** **MSTPGM** **MSTPGMZ**	MVScope Program Virt Stor - Table Data
MSTPGM **MSTPGMZ**	MVScope PSW Sample - Table Data
SYSOVER SYSSUM	Summary - Table Data
PGSPS SWDINFO SWDSTAT SWPINFO	Swap Dataset - Table Data
EXCEPT **SRCS** **SYSCNFG** SYSINFO SYSSTAT **SYSWKLD**	System CPU - Table Data
ESINFO **EXCEPT** EZMSTOR EZMSYS FRMINFO PGINFO **SPAG** **SRCS** STORAGE **SYSCNFG** **SYSWKLD**	System Paging - Table Data
SPAG	System Swap - Table Data
SMSINFO	SMS Storage Group - Table Data
DSPCDUMP	SPData Space - View - Contents
DDMN DMNSTAT DMNSTATR	SRM Domain - Table Data
MSRITEMZ **MSRSRCZ**	MVScope Time Buckets - Table Data
MSRSLICE	MVScope Time 8 Buckets - Table Data
MSMVSTG	MVScope Virtual Storage - Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
MSICCW **MSIOZ** **MSIRESP** **MSISEEK** **MSITRACE** **MSMVOL**	MVScope Volume Extent - Table Data
EZMWBAT EZMWORK EZMWTSO TRX WCPU WCPUR WCPUS WDELAY WDELAYR WDELAYS WDELAYZ WFLOW WFLOWR WFLOWS WFLOWZ WIO WIOR	Workload - Table Data
WMCNVT WMCNVTR WMCNVTRZ WMCNVTZ WMDLY WMDLYR WMDLYRZ WMDLYZ **WMPRD** WMPRDR WMPRDRZ WMPRDZ **WMRCLS** WMRCLSR WMRCLSRZ WMRCLSZ **WMRTD**	Workload - WLM Ext Period - Table Data (MAINVIEW for MVS 2.4.2 and later) (CMF 5.2.3 and later)
WMPRD **WMRCLS** **WMRTD** **WMSCLS** **WMWKLD**	Workload - WLM Period - Table Data (MAINVIEW for OS/390 prior to 2.4.2) (CMF prior to 5.2.3)
WMASSC	Workload - WLM Server - Table Data

Table 32. CMF MONITOR and MAINVIEW for OS/390 Views (Continued)

View	Resource Definition
WMWKM WMWKMZ	Workload - WLM Subsystem - Table Data
XCFMBR XCFMBRR	XCF Member - Table Data
XCFCF XCFCTC XCFPTH XCFPTHR	XCF Path - Table Data
XCFSYS XCFSYSR	XCF System - Table Data

MAINVIEW Alarm Manager Views

Table 33 lists distributed MAINVIEW Alarm Manager views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW Alarm Manager views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of MAINVIEW Alarm Manager.

Table 33. MAINVIEW Alarm Manager Views

View	Resource Definition
ALGBRO01 ALGEDI01 ALGLST01 ALMADD01 ALMBRO01 ALMEDI01 ALMLST01 ALMLST02	Alarm Groups - Table Data
ALGBRO01 ALGEDI01 ALGLST01 ALMADD01 ALMBRO01 ALMEDI01 ALMKEY01 ALMKEY02 ALMLST01 ALMLST02	Alarm Definitions - Table Data
ALGBRO01 ALGEDI01 ALGLST01 ALMADD01 ALMBRO01 ALMEDI01 ALMLST01 ALMLST02	Alarm Thresholds - Table Data
ALARM ALARMH ALARMZ	Alarm Messages - Table Data

MAINVIEW for CICS Views

Table 34 lists distributed MAINVIEW for CICS views and their corresponding resource definitions.

Note: As described in Chapter 15, “Resources Definitions Listed by Product” on page 175Chapter 15, “Resources Definitions Listed by Product” on page 175, you can control access to all MAINVIEW for CICS views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of MAINVIEW for CICS.

Table 34. MAINVIEW for CICS Views

View	Resource Definition
MAIN	Main view - Table Data
SECURITY ADMIN USER MONITOR WORKLOAD REGION	Security view - Table Data
EZCSSI EZCICS EZCFAST EZCMDATA EZCMFILE EZCMNETW EZCMPROG EZCMREGN EZCMSTOR EZCMTASK EZCMUTIL EZCREGN EZCUTILC EZCUTILV EZCRUTIL EZCRUTLC EZCRUTLV	Easy views - Table Data
DSLIST	Historical datasets - Table Data
COBJ COBJR COBJS COBJZ COBJRZ COBJSZ	Workload objectives - Table Data

Table 34. MAINVIEW for CICS Views (Continued)

View	Resource Definition
CFLOW CFLOWS CWOVER CWOVERS CWOVERD CWOVERDS	Response time - Table Data
CREGION CREGOVER CREGIONZ CREGHR CREGDET1 CREGDET2 CREGDET3 CREGDET4 CREGDET5 CREGNSEL	Regions - Table Data
CMAREAZ	Monitors - Table Data by Area
CMON CMONC CMONR CMONS	Monitors - Table Data by Target
CSOVER CSOVERC CSOVERR CSOVERS	Monitors - Table Data by Type
CSERV CSERVC CSERVR CSERVS	Monitors - Table Data by Monitor
CWKLDDEF CWKLDDET	Monitors - Table Data Workload definitions
CAMXT CMXTC C@CMXT	Monitors - Table Data Max Task
CCSUT CECSUT	Monitors - Table Data CSA
CDSUT C#DSAV C#DSIZ C#DSTO	Monitors - Table Data DSA

Table 34. MAINVIEW for CICS Views (Continued)

View	Resource Definition
C#ESAV C#ESIZ C#ESTO C#PROC	Monitors - Table Data ESA
C@SVCT	Monitors - Table Data Storage violations
CLSRL CLSRS CLSRW	Monitors - Table Data LSR
CSDCT CPGMS CTSTE	Monitors - Table Data Storage dumps
C@INPQ C@RESP C@RSTM	Monitors - Table Data Input time
C@ELAP C@ELTM	Monitors - Table Data Elapsed time
C@PICT	Monitors - Table Data Program interrupts
C@GLBD C@GLBE C@GLBM C@GLBP C@GLBT C@GLBU C@GLBX	Monitors - Table Data CICS CPU
C@MONI	Monitors - Table Data CICS exceptions
C@PRB1 C@PRB2 C@PRB3 C@PRB4	Monitors - Table Data CICS Problems
C@TDBU C@TDBW C@TDQL C@TDQT C@TDSU C@TDSW	Monitors - Table Data TD

Table 34. MAINVIEW for CICS Views (Continued)

View	Resource Definition
C@TSBU C@TSBW C@TSSU C@TSSW	Monitors - Table Data TS
C@TSKA C@TSKB C@TSKC C@TSKD C@TSKF C@TSKS	Monitors - Table Data TASK

MAINVIEW for DATA ACCELERATOR Compression Views

Table 35 lists distributed MAINVIEW for DATA ACCELERATOR Compression views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for DATA ACCELERATOR Compression views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of MAINVIEW for DATA ACCELERATOR Compression.

Table 35. MAINVIEW for DATA ACCELERATOR Compression Views

View	Resource Definition
CATLIST	MVS Catalog - Table Data
DACREGI	DAC REGISET Entry Statistics - Table Data
DACSTATS	DAC Compression Statistics - Table Data
IMSSTATS	DPK/IMS Statistics - Table Data
SMSSTATS	SMS Dataset Statistics - Table Data

MAINVIEW for DB2 Views

Table 36 lists distributed MAINVIEW for DB2 views (x indicates a group of views) and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for DB2 views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW for DB2 security parameter member.

Table 36. MAINVIEW for DB2 Views

View	Resource Definition
DMAREAZ DMONx DMWARN DSERVx DSOVERx	Monitor - Table Data
Dxxxxx (all monitor plot views)	Monitor - Table Data
DOBJxx	Appl Workload - Table Data
STxxxxxx	Status - Table Data
WZxxxxxx	Status - Table Data BufferPool - Table Data
BFRxxxxx GBPxxxxx	BufferPool - Table Data
PSxxxxxx	IoActivity - Table Data
LKxxxxxx	LockOuts - Table Data
THDxxxxx	Users - Table Data
ZPxxxxxx	ZPARM - Table Data

MAINVIEW Explorer Views

Table 37 lists distributed MAINVIEW Explorer views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW Explorer views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of MAINVIEW Explorer.

Table 37. MAINVIEW Explorer Views

View	Resource Definition
CLIENTS	SessionInfo - Table Data
EZEXP	ViewTable - Table Data
HSINFO	ServerInfo - Table Data
MVXVIEWS	ViewTable - Table Data

MAINVIEW for IMS Views

Table 38 lists distributed MAINVIEW for IMS views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for IMS views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW for IMS security parameter member.

Table 38. MAINVIEW for IMS Views

View	Resource Definition
ISOVERC IMONC ISERVC ISOVER IMON ISERV ISOVERR IMONR ISERVR ISOVERS IMONS ISERVS IWKLDDEF IWKLDDET IMFSIO IMFSIR IMFSFD	Monitor - Table Data
IINQTR IINQCL IIQSCL IOQLT IOQLN IOQND IOUTLT IOUTLN IOUTND IOQLK IOUTLK IINLK IDEADQ IARVBG IARVTR IARVCL IARVPR	Monitor - Table Data, continued

Table 38. MAINVIEW for IMS Views (Continued)

View	Resource Definition
IDBSTL IDBHIT ISBUSE IVDBIO IVDBWR IVHIT IHPACC IHPHIT IHPSTL IPOOLA IPOOLN IPOOLT ILAWT IDSAP ICIOP ICWAP	Monitor - Table Data, continued
IWKAP IPSBW IDBWP IPSBP IDMBP IHIOP IRECA IEPCB IOBUFW IOCHKW IWADIO IPAGE IDPAGE ICSAUT IECSAU IDLIO ISYSIO	Monitor - Table Data, continued

Table 38. MAINVIEW for IMS Views (Continued)

View	Resource Definition
ILDLCK ILHELD ILKREQ ILSUSP ILTMOT IPTBLK IVSEND I@INPQ I@ELAP I@RESP I#PROC I@OBA I#OBAW I#CIC I@PDB2 I#CDB2 I#SDB2	Monitor - Table Data, continued
IOBJ IOBJR	Appl Workload - Table Data
IMSPLXR IMSPLX IMSPLXGR IMSPLXG IMSPLSR IMSPLS IMSPLSGR IMSPLSG IMSDTLGR IMSDTLG IMSDTLR IMSDTL IMSPLMR IMSPLM IMSPLMGR IMSPLMG	IMS Overview - Table Data
IRGOVWR IRGOVW IRGOCCR IRGOCC IRGOCCGR IRGOCCG	Region Occupancy - Table Data

Table 38. MAINVIEW for IMS Views (Continued)

View	Resource Definition
ICLSUMR ICLSUM ICLSUMGR ICLSUMG ICLSUMSR ICLSUMS ICLSUGSR ICLSUGS ICLSUMMR ICLSUMM ICLSUGMR ICLSUGM ICLDTLR ICLDTL	Class Activity - Table Data
ITRSUMR ITRDTLR	Transaction - Table Data
IBGSUMR IBGSUM	Balancing Group - Table Data
ISAMPOP ISAMPOPD	Sampler Operation - Table Data
IFCTR IFCTRA IFCTRD IFCTRI IFCTRP IFCTRQ IFCTRR IFCTRS IFCTR2 IDLTR IDLTRIO IDLTRPL IDLTROT IDLDB IDLDBC IDLDBD IDLDBI	Tran Sample Event - Table Data

Table 38. MAINVIEW for IMS Views (Continued)

View	Resource Definition
IDLDB IDLDBC IDLDBD IDLDBI IDLDBP IDLDBTR IDLDBV IDLDD IDLDDC IDLDDI IDLDDP IDLDDTR IDLDDV IDLVL IDLVLC IDLVLI IDLVLP	Tran I/O - Table Data
IDLTRLK IDLLK IDLLKC IDLLKI IDLLKP IDLLKTR	Tran Lock - Table Data
IDLLHTR IDLLH IDLLHC IDLLHI IDLLHP IDLTRLH	Tran Latch - Table Data

MAINVIEW for IP Views

Table 39 lists distributed MAINVIEW for IP views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for IP views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of MAINVIEW for IP.

Table 39. MAINVIEW for IP Views

View	Resource Definition
ALLCONS ALLDET CLSACONS CLSBCONS CLSCCONS CLSARESP CLSBRESP CLSCRESP CONNRESP	Connections - Table Data
EZIP EZIPCONF EZIPCONS EZIPRESP	Menu - Table Data
IPCONF IPCONFD	Configuration - Table Data
JOBRESP JOBRESPD JOBRESPS	Job Response - Table Data
PORTRSPP PORTRSPD PORTRSPS	Port Response - Table Data
SMFCONF SMFCONFD	Configuration - Table Data
TACAPPL TACAPPLD	Connections - Table Data
TACDEVD TACDEVS	Network Devices - Table Data
TACLNKD TACLNKS	Network Links - Table Data
TACPORT TACPORTD	Ports - Table Data
TACROUT TACROUTD	Routes - Table Data

Table 39. MAINVIEW for IP Views (Continued)

View	Resource Definition
TACTCSB	Stack Information - Table Data
TCPCONF TCPCONFD	Configuration - Table Data
TCPCONS TCPDET	Connections - Table Data
UDPCONF UDPCONFD	Configuration - Table Data
UDPCONS UDPDET	Connections - Table Data

MAINVIEW for MQSeries Views

Table 40 lists distributed MAINVIEW for MQSeries views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for MQSeries views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW for MQSeries security parameter member.

Table 40. MAINVIEW for MQSeries Views

View	Resource Definition
AQ AQD	Alias Queue - Table Data
CHNLS CHNLAD CHNLST	Channel - Table Data
CCHNL CCHNLD	CICSChnl - Table Data
LQM DLQM LQMD DLQMD XQM MB XQMD ML MLX EVTXMIT EVTQM EVTQ EVTQS EVTBR EVTUO EVTAB EVTCH	Message - Table Data
MQ MQD	ModelQueue - Table Data
PROC PROCD THRDA THRDI THRDZ PS STC STCD	Processes - Table Data

Table 40. MAINVIEW for MQSeries Views (Continued)

View	Resource Definition
LQ LQD XQ	Queue - Table Data
QUEUES	Queue List - Table Data
QMPROF QMDEF QMDEFDM QMPROFDM QMDEFDR QMPROFDR	QMgrDef - Table Data
RQ RQD	Remote Queue - Table Data
TOPOLOGY TOPLIST TOPEXCP TOPOVER BP BPD	Topology - Table Data
BP BPD	BufPool - Table Data
PS	PageSet - Table Data
STC STCD	StorageClass - Table Data
THRDA THRDI THRDZ	Thread - Table Data

MAINVIEW SYSPROG Services Views

Table 41 lists distributed MAINVIEW SYSPROG Services views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW SYSPROG Services views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of MAINVIEW SYSPROG Services.

Table 41. MAINVIEW SYSPROG Services Views

View	Resource Definition
CONSOLE	MVSPS Consoles - Table Data
CONSOLES	MVSPS Consoles List - Table Data
EMSTAT	MVSPS Sys Intvl - Table Data
WARN	MVSPS Warning - Table Data

MAINVIEW for UNIX System Services Views

Table 42 lists distributed MAINVIEW for UNIX System Services views and their corresponding resource definitions. Views in **BOLD** face type require you to secure more than one resource table.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for UNIX System Services views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW for UNIX System Services security parameter member.

Table 42. MAINVIEW for UNIX System Services Views

View	Resource Definition
BPXPRM IPCBPXP	System Parameters - Table Data
ASINFO **ASDELAYZ** **ASOVERZ**	WLM Address Space - Table Data
DCSTAT	Data Collect Stat - Table Data
FSINFO **FSMOUNT** **FSMOUNTZ** **HFSINFO** **HFSOVERZ** **HFSOVER** **HFSIOZ** **HFSIO**	Filesystems Mounted - Table Data
FSPACE FSFILENM FSDIRNM	File Space Usage - Table Data
FSINFO FSMNTPT **FSMOUNT** **FSMOUNTZ** **HFSINFO** **HFSOVERZ** **HFSOVER** **HFSIOZ** **HFSIO**	Filesys/mountpoint - Table Data

Table 42. MAINVIEW for UNIX System Services Views (Continued)

View	Resource Definition
FSINFO FSMNTPRM **FSMOUNT** **FSMOUNTZ** **HFSINFO** **HFSOVERZ** **HFSOVER** **HFSIOZ** **HFSIO**	Filesys/mountparm - Table Data
HFSGBUF HFSGBUFZ	HFS Global Buffers - Table Data
HFSGINFO	HFS Global - Table Data
HFSINFO **HFSIOZ** **HFSIO** **HFSOVERZ** **HFSOVER**	HFS Filesystem - Table Data
ASDELAYZ **ASOVERZ** **GRPOVERZ** **PSCMND** **PSOVER** **PSOVERZ** **PSUSE** **PSUSEZ** **PSDELAY** **PSDELAYZ** **PSINFO** **PSSTAT** **PSTREE** **USROVERZ** **USRSESSZ**	Process - Table Data
ASDELAYZ **ASOVERZ** **GRPOVERZ** PSCTTY **PSCMND** **PSOVER** **PSOVERZ** **PSUSE** **PSUSEZ** **PSDELAY** **PSDELAYZ** **PSINFO** **PSSTAT** **PSTREE** **USROVERZ** **USRSESSZ**	Process/tty - Table Data

Table 42. MAINVIEW for UNIX System Services Views (Continued)

View	Resource Definition
ASDELAYZ **ASOVERZ** **GRPOVERZ** **PSCMND** PSCMDPRM **PSDELAY** **PSDELAYZ** **PSINFO** **PSOVER** **PSOVERZ** **PSUSE** **PSUSEZ** **PSSTAT** **PSTREE** **USROVERZ** **USRSESSZ**	Process/command - Table Data
ASDELAYZ **ASOVERZ** **GRPOVERZ** **PSCMND** **PSDELAY** **PSDELAYZ** PSEXPATH **PSINFO** **PSOVER** **PSOVERZ** **PSUSE** **PSUSEZ** **PSSTAT** **PSTREE** **USROVERZ** **USRSESSZ**	Process/path - Table Data
ASDELAYZ **ASOVERZ** **GRPOVERZ** **PSCMND** **PSDELAY** **PSDELAYZ** **PSINFO** **PSOVER** **PSOVERZ** **PSUSE** **PSUSEZ** PSWRKDIR **PSSTAT** **PSTREE** **USROVERZ** **USRSESSZ**	Process/cwd - Table Data

Table 42. MAINVIEW for UNIX System Services Views (Continued)

View	Resource Definition
PSFOPEN PSFILENM	Process Files Open - Table Data
PSTREE	Process Tree - Table Data
REQSTAT	Request Status - Table Data

MAINVIEW VistaPoint Views

Table 43 lists distributed MAINVIEW VistaPoint views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW VistaPoint views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW VistaPoint security parameter member.

Table 43. MAINVIEW VistaPoint Views

View	Resource Definition
APGRP APGRPC APGRPR APGRPS APOVER APOVERC APOVERR APOVERS WKDETL WKDETLC WKDETLR WKDETLS WKOVER WKOVERC WKOVERR WKOVERS	Appl Workload - Table Data
APPLDEF APPLDEFZ	Appl Definition - Table Data
VMON VMONC VMONR VMONS	Monitor - Table Data

MAINVIEW for VTAM Views

Table 44 lists distributed MAINVIEW for VTAM views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for VTAM views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW for VTAM security parameter member.

Table 44. MAINVIEW for VTAM Views

View	Resource Definition
APPLAV APPLAVD APPLCON APPLCOND APPLCONS APPLS APPLDET APPLSUM ARES ARESDET ARESUM	Applications - Table Data
EZAPPL EZLU EZTN3270 EZTRAN EZVTAM	Menu - Table Data
LURES LURESDET LURESUM	LU Resources - Table Data
LUS LUDET LUSUM	LUs - Table Data
NCPINFO	SOPNCP - Table Data
NCPRINFO	SOPRSC - Table Data
TAPPCORR TDOMAIN TIPADDR TIPLUMAP TLUBYTED TLUS TRESPDOM TRESPIPA TRESPLU TRESPLUD	TN3270 Statistics - Table Data
VTMBUFF	SOPBfuse- Table Data

Table 44. MAINVIEW for VTAM Views (Continued)

XACTNS XACTDET XACTSUM	Transactions - Table Data
XACTRES XACTRESD XACTRSUM	Transaction Resources - Table Data

MAINVIEW for WebSphere Views

Table 45 lists distributed MAINVIEW for WebSphere views and their corresponding resource definitions.

Note: As described in Chapter 15, "Resources Definitions Listed by Product" on page 175, you can control access to all MAINVIEW for WebSphere views collectively by enabling, disabling, or changing the `Default - Table Data` in the SERDEF view of the MAINVIEW for WebSphere security parameter member.

Table 45. MAINVIEW for WebSphere Views

View	Resource Definition
ACCESS ACCESSD ACCESSZ AUTHZ	Access - Table Data
ACCSTAT	Hourly Access - Table Data
CACHE CACHED	Web Server Information - Table Data
CODEZ	Access - Table Data
ERRORS ERRORSD ERRORSZ	Errors - Table Data
ERRSTAT	Hourly Errors - Table Data
EZAAUTH EZERRORZ EZFILE EZFILNF EZHACC EZHERR EZHUSR EZVUSR EZWEB	Menu - Table Data
FILESUM NOFILEZ	Access - Table Data
PERFORM PERFORMD PERFSUM REQUEST REQUESTD RESPONSE RESPONSD SERVER	Web Server Information - Table Data
STMDATA STMDATAD	Client Response Times - Table Data

Table 45. MAINVIEW for WebSphere Views (Continued)

TRAFFIC TRAFFICD	Web Server Information - Table Data
UACCSUM UVOLSUM	Access - Table Data

Part 4. MAINVIEW Alternate Access Security

This part describes MAINVIEW Alternate Access security.

Chapter 17. Defining Security for MAINVIEW Alternate Access 305
Understanding AutoLogon Session Security Issues 305
Defining Additional Security for Terminals 306
Defining Additional Security for Applications 307
Configuring CA-ACF2 for MAINVIEW Alternate Access 308
Customizing Class TERMINAL Access Authorization for CA-ACF2 311
Customizing Class APPL Access Authorization for CA-ACF2 311
Configuring RACF for MAINVIEW Alternate Access 313
Customizing Class TERMINAL Access Authorization for RACF 314
Customizing Class APPL Access Authorization for RACF 314
Configuring CA-TOP SECRET for MAINVIEW Alternate Access 315
Customizing Class TERMINAL Access Authorization for CA-TOP SECRET 316
Customizing Class APPL Access Authorization for CA-TOP SECRET 317

Chapter 17. Defining Security for MAINVIEW Alternate Access

MAINVIEW Alternate Access uses the standard MVS SAF interface to interface with your external security manager (ESM) and requires that each user ID for a session be defined to your ESM. A session does not initialize if the user ID is unknown to your ESM.

Other customization to support security may be required as well, depending on which ESM is installed at your site. For example:

- AutoLogon sessions may be established with user IDs that do not require manual entry of clear text passwords by customizing CA-ACF2 or RACF to define and protect a `FACILITY(BOOLEBBV)` resource or CA-TOP SECRET to define and protect an `IBMFAC(BOOLEBBV)` resource.
- By using a `FACILITY(BOOLEBBV)` or `IBMFAC(BOOLEBBV)` resource, sessions can be further restricted to be used only at specifically authorized terminals or only with MAINVIEW Alternate Access.

  This type of customization eliminates any potential security exposure resulting from removing the requirement for manual entry of a clear text password.

This chapter discusses the security issues concerning MAINVIEW Alternate Access sessions and how to configure CA-ACF2 or RACF to support the `FACILITY(BOOLEBBV)` resource or CA-TOP SECRET to support an `IBMFAC(BOOLEBBV)` resource in the following sections:

- "Understanding AutoLogon Session Security Issues"
- "Defining Additional Security for Terminals" on page 306
- "Defining Additional Security for Applications" on page 307
- "Configuring CA-ACF2 for MAINVIEW Alternate Access" on page 308
- "Configuring RACF for MAINVIEW Alternate Access" on page 313
- "Configuring CA-TOP SECRET for MAINVIEW Alternate Access" on page 315

Understanding AutoLogon Session Security Issues

AutoLogon sessions sign on a terminal directly to a product service at terminal address space (TAS) initialization, without requiring user intervention to enter a user ID or password.

AutoLogon sessions can be passed through to an application because the OPT( ) subparameter is passed at session initialization. For a session to initialize properly to support the OPT( ) subparameter, user ID and password (if required) values must be defined as startup parameters for the session. Because AutoLogon sessions require user ID and password values as startup parameters, security considerations dictate special procedures to prevent the unnecessary exposure of these values.

There are two ways to provide the user ID and a password at AutoLogon session initialization:

- in the START command
- in a BBVTAS*xx* member

When the `FACILITY(BOOLEBBV)` or `IBMFAC(BOOLEBBV)` resource has not been defined to your ESM, the user ID and password must be manually specified in clear text in either the

START command or the BBVTAS*xx* member. Specifying the user ID and a password in clear text presents three potential security problems:

- The user ID and password are visible on the console when specified in a START command.
- The entire START command may be logged to SYSLOG when issued, making the user ID and password values visible in SYSLOG.
- The user ID and password are visible in a BBVTAS*xx* member, which may be accessible by many other individuals.

To avoid the problem of clear-text password exposure for user IDs that are to be used with AutoLogon sessions, BMC Software recommends the following two solutions:

- Define all BBVTAS*xx* members containing user ID or password values in a read-secured data set. This solution additionally requires that
  - a separate TAS procedure be defined (see Step 6: Define a Startup Procedure for a TAS, in the *MAINVIEW Alternate Access Implementation and User Guide*) that concatenates the read-secured data set to the BBVPARM DD statement in the procedure
  - the user ID to be used by the TAS when it is started be given access to this read-secured data set
- Define the resource `FACILITY(BOOLEBBV)` to ACF2 or RACF or the `IBMFAC(BOOLEBBV)` resource to TOP SECRET to eliminate the requirement to code clear text passwords for IDs that are authorized to access this resource.

Defining Additional Security for Terminals

MAINVIEW Alternate Access passes environmental information, such as the `TERMID=` parameter, to the ESM through RACROUTE to enable the installation to further restrict access.

The `TERMID=` parameter is an optional parameter that is specified in the RACROUTE VERIFY (signon) parameter list. The `TERMID=` is the VTAM LU or EXCP terminal address from which a MAINVIEW Alternate Access logon is being attempted. If the terminal is protected and the user ID is not allowed access from the terminal, the logon terminates after an error message is issued.

For RACF and CA-TOP SECRET, all VTAM LUs or addresses are protected using class `TERMINAL`. For CA-ACF2, terminal access authorization is handled through standard CA-ACF2 terminal/source group restrictions.

Specific examples for defining resources in class `TERMINAL` are provided in the following sections:

- “Customizing Class TERMINAL Access Authorization for CA-ACF2” on page 311
- “Customizing Class TERMINAL Access Authorization for RACF” on page 314
- “Customizing Class TERMINAL Access Authorization for CA-TOP SECRET” on page 316

Defining Additional Security for Applications

MAINVIEW Alternate Access passes environmental information, such as the `APPL=` parameter, to the ESM through RACROUTE to enable the installation to further restrict access. To use application names to control access to MAINVIEW Alternate Access, each application name must be defined as a resource in class `APPL`.

There are two instances where MAINVIEW Alternate Access uses resources in SAF class `APPL` to control access to MAINVIEW Alternate Access:

- The first instance is when the user ID attempting MAINVIEW Alternate Access logon is validated. This instance is intended to offer protection at the application level. The `APPL=` parameter is an optional parameter that is specified in the RACROUTE VERIFY (signon) parameter list. In this case, an application name of BBVLOGON is passed as the `APPL=` parameter when MAINVIEW Alternate Access validates the user ID. The security system uses this parameter automatically to validate application access.

  If the installation wants to restrict MAINVIEW Alternate Access to only a certain subset of users, the resource entity name `BBVLOGON` in SAF resource class `APPL` may be defined. The ESM ensures, as part of user ID validation, that the user ID has at least read access to the `BBVLOGON` resource in class `APPL`. For CA-ACF2, SAF resource class `APPL` is usually mapped to a unique generalized resource rule type; the default for CA-ACF2 6.*x* is `TYPE(APL)`.

- The second instance is designed to offer protection at MAINVIEW for OS/390 node name level. Once the user ID has been validated (and access to the BBVLOGON application validated), BBV explicitly invokes the ESM to authorize access to a resource in SAF class `APPL` whose resource entity name is the VTAM major node name.

  By controlling access to the VTAM major node name, the installation can, for example, allow a user to log on to MAINVIEW Alternate Access on specific MVS images only, or to log on to a test version of MAINVIEW Alternate Access, but not to a production version. For these examples to function as illustrated, the VTAM major node names used for MAINVIEW Alternate Access must be unique across different MVS images or between production and test versions.

  Note: The VTAM major node name referred to here is the value specified for the `APPLID=` parameter in the BBVLAS*xx* member in *hilevel*.*sysid*UBBPARM.

When the MAINVIEW Alternate Access session is not using VTAM, but is instead an EXCP session, the constant, `BBVEXCP`, is used for the resource entity name instead of a VTAM major node name. Specific examples for defining resources in class `APPL` are provided in the following sections:

- "Customizing Class APPL Access Authorization for CA-ACF2" on page 311
- "Customizing Class APPL Access Authorization for RACF" on page 314
- "Customizing Class APPL Access Authorization for CA-TOP SECRET" on page 317

Configuring CA-ACF2 for MAINVIEW Alternate Access

The following customization is required to

- define LOGONIDs for appropriate MAINVIEW Alternate Access started tasks and a `FACILITY(BOOLEBBV)` resource
- allow access to the resource for LOGONIDs associated with user IDs to be used in AutoLogon sessions

Contact your CA-ACF2 system programmer or security administrator for help.

1. Define a LOGONID for the BBVTAS started task. This LOGONID is used during the initial phase of startup. The user's LOGONID is used for the session once the session initializes; therefore, users do not require additional or separate LOGONIDs to use MAINVIEW Alternate Access.

   Note: The started task LOGONID requires access to the BMC Software product data sets.

   Define the LOGONID with the following attributes:

   ```
   DUMPAUTH
   STC
   RESTRICT
   SOURCE(STCINRDR)
   ```

2. This optional step requires an IPL of your system. This step may not be applicable to your site.

   If you use the ACF2 started task validation exit to assign a LOGONID to a started task:

   a. Add the LOGONID for the BBVTAS started task to the exit.

   b. Assemble and relink the exit.

   c. IPL your system to activate the revised exit.

3. Repeat the previous two steps for the BBVLAS started task, if necessary.

4. For CA-ACF2 5.2, update your CA-ACF2 SAFPROT list to include a control point for BBVTLOAD.

   The following example shows a set of TSO commands to perform this update:

   ```
   ACF
   SET CONTROL(GSO)
   INSERT SAFPROT.BBV CLASSES(-)  CNTLPTS(-) SUBSYS(BBVTLOAD)
   END
   ```

   For CA-ACF2 6.*x*, define a SAFDEF record for BBVTLOAD.

   The following example shows a set of TSO commands to perform this update:

   ```
   ACF
   SET CONTROL(GSO)
   INSERT SAFDEF.BBVTLOAD ID(BBVTLOAD) +
          MODE(GLOBAL) REP +
          RACROUTE(SUBSYS=BBVTLOAD,REQSTOR=-)
   END
   ```

5. For CA-ACF2 5.2, perform a CA-ACF2 refresh of the SAFPROT list.

   Use the following operator command to refresh the SAFPROT list:

   ```
   F ACF2,REFRESH(SAFPROT)
   ```

   For CA-ACF2 6.*x*, perform a CA-ACF2 refresh of the SAFDEF records.

   Use the following operator command to refresh all the SAFDEF records:

   ```
   F ACF2,REFRESH(SAFDEF)
   ```

6. For CA-ACF2 5.2, optionally define a mapping between the SAF resource class `FACILITY` and a CA-ACF2 generalized resource rule of any type. If you define this mapping on CA-ACF2 5.2, you must update the SAFMAPS GSO record and refresh the in-storage SAFMAPS table.

   a. The following example shows a set of TSO commands to update the SAFMAPS GSO record for CA-ACF2 5.2, assuming you selected the generalized resource rule type `FAC`:

      ```
      ACF
      SET CONTROL(GSO)
      CHANGE SAFMAPS ADD MAPS(FAC/FACILITY)
      END
      ```

   b. Use the following operator command to refresh the in-storage SAFMAPS table for CA-ACF2 5.2:

      ```
      F ACF2,REFRESH(SAFMAPS)
      ```

      For CA-ACF2 6.*x*, the SAF resource class `FACILITY` is mapped automatically to the generalized resource rule type `FAC`, so no action is required.

7. Some MVS components may require that the rules for the rule type selected for use with SAF class `FACILITY` be resident. If you need to perform this customization:

   - And you have already migrated to the INFODIR record for either CA-ACF2 6.*x* or for CA-ACF2 5.2, update the INFODIR GSO record, refresh the INFODIR information in storage, and build the in-storage directory for the selected rule type.

     a. The following example shows a set of TSO commands to add rule type `FAC` to the INFODIR GSO record:

        ```
        ACF
        SET CONTROL(GSO)
        CHANGE INFODIR ADD TYPES(R-RFAC)
        END
        ```

     b. Use the following operator command to refresh the INFODIR data:

        ```
        F ACF2,REFRESH(INFODIR)
        ```

     c. Use the following operator command to build the in-storage directory for the rule type `FAC`:

        ```
        F ACF2,REBUILD(FAC)
        ```

   - And your CA-ACF2 5.2 configuration uses the RESDIR GSO record instead of the INFODIR GSO record, update the RESDIR GSO record and refresh the RESDIR

information in storage for the selected rule type. This will add rules of type FAC to the list from which in-storage directories are built at CA-ACF2 initialization.

a. The following example shows a set of TSO commands to add rule type FAC to the RESDIR GSO record:

```
CHANGE RESDIR ADD TYPES(R-FAC)
```

b. Use the following operator command to refresh the RESDIR data:

```
F ACF2,REFRESH(RESDIR)
```

8. Define a BOOLEBBV rule of type SAF or the type selected in Step 7 on page 309 and permit access to the rule for each LOGONID to be used with an AutoLogon session. This step allows LOGONIDs to skip the requirement to enter a clear text password manually.

a. The following example shows a set of TSO commands to add a BOOLEBBV rule to the rule type FAC:

```
ACF
SET RESOURCE(FAC)
COMPILE * LIST STORE
$KEY(BOOLEBBV) TYPE(FAC)
  UID(UID string) ALLOW
  UID(-) PREVENT
END
END
```

The following example shows how these commands might be defined for specific LOGONIDs:

```
ACF
SET RESOURCE(FAC)
COMPILE * LIST STORE
$KEY(BOOLEBBV) TYPE(FAC)
$USERDATA( RESOURCE RULE TO ALLOW BBV AUTOLOGON )
  UID(152911131) ALLOW
  UID(155311115) ALLOW
  UID(155311117) ALLOW
  UID(155311119) ALLOW
  UID(333333333) ALLOW
  UID(-) PREVENT
END
END
```

b. If the rule type is defined as resident, use the following operator command to rebuild the in-storage directory for the rule type FAC:

```
F ACF2,REBUILD(FAC)
```

Customizing Class TERMINAL Access Authorization for CA-ACF2

ACF2 support of the `TERMID=` parameter in the RACROUTE VERIFY parameter list is handled by standard CA-ACF2 source and source group restriction.

To authorize the LOGONID for system entry using MAINVIEW Alternate Access at a specific terminal, that terminal's VTAM LU name or EXCP address must appear in a source group whose name is specified by the SOURCE attribute for the LOGONID.

Customizing Class APPL Access Authorization for CA-ACF2

For CA-ACF2 support of MAINVIEW Alternate Access application authorization using the `APPL=` parameter in the RACROUTE VERIFY parameter list and VTAM major node name access authorization, review the following steps and perform any actions necessary for your installation:

1. For CA-ACF2 6.0 and later, you must define an additional SAFDEF record. The following TSO commands may be used to define the new record:

   ```
   ACF
   SET CONTROL(GSO)
   INSERT SAFDEF.BBVTLOAD ID(BBVTAPPL) MODE(GLOBAL) REP +
          RB(BBVTLOAD) PROGRAM(BBVTLOAD) +
          RACROUTE(REQUEST=AUTH,CLASS=APPL)
   END
   ```

   Then, issue the following operator command to refresh the SAF definitions in storage:

   ```
   F ACF2,REFRESH(SAFDEF)
   ```

2. Determine the generalized resource rule type that SAF resource class `APPL` has been mapped to:

   – For CA-ACF2 5.2, this is defined by the SAFMAPS GSO records
   – For CA-ACF2 6.0 and later, this is defined by a CLASMAP GSO record

   By default, SAF resource class `APPL` is mapped to resource type SAF. You may map class `APPL` to any generalized resource rule type. If you use a rule type other than SAF, you must add an entry to the SAFMAPS GSO record for CA-ACF2 5.2 or define an additional CLASMAP GSO record for CA-ACF2 6.0 and later.

   Note: In the subsequent examples, the assumption is made that the SAF resource class `APPL` has already been mapped to the generalized resource rule type `APL`.

3. For CA-ACF2 5.2, if desired, update the SAFMAPS GSO record to map resource class `APPL` to rule type APL, for example.

   The following TSO commands may be used to update the existing SAFMAPS record:

   ```
   ACF
   SET CONTROL(GSO)
   CHANGE SAFMAPS ADD MAPS(APL/APPL)
   END
   ```

   Then, issue the following operator command to refresh the SAFMAPS table in storage:

   ```
   F ACF2,REFRESH(SAFMAPS)
   ```

4. For CA-ACF2 6.*x*, if desired, add a new CLASMAP GSO record that maps resource class `APPL` to rule type APL, for example. The following TSO commands may be used to define the new record:

   ```
   ACF
   SET CONTROL(GSO)
   INSERT CLASMAP.APPL RSRCTYPE(APL) RESOURCE(APPL) ENTITYLN(8)
   END
   ```

   Then, issue the following operator command to refresh the external CLASMAP table in storage:

   ```
   F ACF2,REFRESH(CLASMAP)
   ```

5. Define a rule for resource `BBVLOGON` in type APL (for example) and specify READ(ALLOW) for each LOGONID that needs to log on to MAINVIEW Alternate Access. For example, you may use the following sample TSO commands:

   ```
   ACF
   SET RESOURCE(APL)
   COMPILE * LIST STORE
   $KEY(BBVLOGON) TYPE(APL)
    UID(-)        PREVENT
    UID(bbv-user) ALLOW
   END
   ```

6. For EXCP sessions only, define a rule for resource `BBVEXCP` in type APL (for example) and specify READ(ALLOW) for each LOGONID that needs to log on to MAINVIEW Alternate Access. For example, you may use the following sample TSO commands:

   ```
   ACF
   SET RESOURCE(APL)
   COMPILE * LIST STORE
   $KEY(BBVEXCP)  TYPE(APL)
    UID(-)        PREVENT
    UID(bbv-user) ALLOW
   END
   ```

7. For each VTAM major node name to be used with MAINVIEW Alternate Access, define a rule in type APL (for example) whose resource name matches the VTAM major node name and specify READ(ALLOW) for each LOGONID that needs to log on to MAINVIEW Alternate Access using a VTAM terminal. For example, you may use the following sample TSO commands:

   ```
   ACF
   SET RESOURCE(APL)
   COMPILE * LIST STORE
   $KEY(lu-name)  TYPE(APL)
    UID(-)        PREVENT
    UID(bbv-user) ALLOW
   END
   ```

8. Rebuild the resident CA-ACF2 resource directory for resource type APL (for example), if necessary. Use the following sample operator command:

   ```
   F ACF2,REBUILD(APL)
   ```

Configuring RACF for MAINVIEW Alternate Access

For RACF support of the `FACILITY(BOOLEBBV)` resource, the following customization is required. Contact your RACF system programmer or security administrator for help.

1. Define a generalized resource profile in class `FACILITY` with an entity name of `BOOLEBBV`. The universal access authority of this entity should be `NONE`.

   The following is a sample RACF (TSO) command to add a `BOOLEBBV` entity to class `FACILITY`:

```
RDEFINE FACILITY  (BOOLEBBV)  UACC(NONE)
```

Important

If you have previously defined a generic profile that covers entity name `BOOLEBBV` but does not specify `NONE` as the universal access, you must perform this step. Unless a universal access of `NONE` is specified, any user ID can sign on through MAINVIEW Alternate Access without specifying a password.

2. Permit each USERID to be used with an AutoLogon session to have READ access to resource `FACILITY(BOOLEBBV)`.

   The following example shows a RACF (TSO) command to permit each USERID:

```
PERMIT BOOLEBBV CLASS(FACILITY) ID(userID) ACCESS(READ)
```

3. List the `BOOLEBBV` profile to ensure that the access list is correct and complete.

   Use the following sample RACF (TSO) command to list the access list:

```
RLIST FACILITY BOOLEBBV ALL
```

4. If necessary, activate the `FACILITY` resource class.

   Use the following sample RACF (TSO) command to activate `FACILITY`:

```
SETROPTS CLASSACT(FACILITY)
```

5. If necessary, refresh any in-storage generic or RACLISTed profiles associated with the `FACILITY` resource class.

   – Use the following sample RACF (TSO) command to refresh in-storage generic profiles:

```
SETROPTS REFRESH GENERIC(FACILITY)
```

   – Use the following sample RACF (TSO) command to refresh in-storage RACLISTed profiles:

```
SETROPTS REFRESH RACLIST(FACILITY)
```

Customizing Class TERMINAL Access Authorization for RACF

For RACF support of terminal access authorization through the `TERMID=` parameter in the RACROUTE VERIFY parameter list, review the following steps and perform any actions necessary for your installation:

1. Define the terminal ID (VTAM LU name or EXCP terminal address) as a protected resource to RACF in class `TERMINAL` by using the following sample command:

   ```
   RDEFINE TERMINAL (terminal-id) UACC(NONE)
   ```

2. Permit each USERID that can log on from this terminal (LUname or address) using the following sample command:

   ```
   PERMIT terminal-id CLASS(TERMINAL) ID(userid) ACCESS(READ)
   ```

3. List the profile to ensure that the access list is correct and complete using the following sample command:

   ```
   RLIST TERMINAL terminal-id ALL
   ```

4. If necessary, activate the `TERMINAL` resource class by using the following sample command:

   ```
   SETROPTS CLASSACT(TERMINAL)
   ```

5. If necessary, refresh the in-storage RACLISTed profiles for the `TERMINAL` class by using the following sample command:

   ```
   SETROPTS REFRESH RACLIST(TERMINAL)
   ```

Customizing Class APPL Access Authorization for RACF

For RACF support of MAINVIEW Alternate Access application access authorization through the `APPL=` parameter in the RACROUTE VERIFY parameter list or through the VTAM major node name, review the following steps and perform any actions necessary for your installation:

1. Define the profile BBVLOGON in class `APPL` to RACF using the following sample command:

   ```
   RDEFINE APPL (BBVLOGON) UACC(NONE)
   ```

2. If EXCP terminal sessions are to be used with MAINVIEW Alternate Access, also define the profile BBVEXCP in class `APPL` to RACF using the following sample command:

   ```
   RDEFINE APPL (BBVEXCP)  UACC(NONE)
   ```

3. Define a profile to RACF in class `APPL` for each VTAM major node name to be used with MAINVIEW Alternate Access using the following sample command:

   ```
   RDEFINE APPL (major-node-name) UACC(NONE)
   ```

4. Permit each USERID that needs to log on to MAINVIEW Alternate Access to have READ access to the `BBVLOGON` resource in class `APPL`.

   For example, you may use the following sample command:

   ```
   PERMIT BBVLOGON CLASS(APPL) ID(userid) ACCESS(READ)
   ```

5. Permit each USERID that needs to log on to MAINVIEW Alternate Access using an EXCP session to have READ access to the `BBVEXCP` resource in class `APPL`.

   For example, you may use the following sample command:

   ```
   PERMIT BBVEXCP CLASS(APPL) ID(userid) ACCESS(READ)
   ```

6. Permit each USERID that needs to log on to MAINVIEW Alternate Access using a VTAM terminal to have READ access to the profile in class `APPL` whose name matches the major node name to be used by MAINVIEW Alternate Access.

   For example, you may use the following sample command:

   ```
   PERMIT major-node-name CLASS(APPL) ID(userid) ACCESS(READ)
   ```

7. List the profiles to ensure that the access list is correct and complete using the following sample commands:

   ```
   RLIST APPL BBVLOGON ALL
   RLIST APPL BBVEXCP ALL
   RLIST APPL major-node-name ALL
   ```

8. If necessary, activate the `APPL` resource class by using the following sample command:

   ```
   SETROPTS CLASSACT(APPL)
   ```

9. If necessary, refresh the in-storage RACLISTed profiles for the `APPL` class by using the following sample command:

   ```
   SETROPTS REFRESH RACLIST(APPL)
   ```

Configuring CA-TOP SECRET for MAINVIEW Alternate Access

For CA-TOP SECRET (TSS) support of the `IBMFAC(BOOLEBBV)` resource, the following customization is required. Contact your CA-TOP SECRET system programmer or security administrator for help.

1. Create a separate TSS facility for MAINVIEW Alternate Access.

   Use the following sample TSS (TSO) commands and TSSPARM updates to create a separate CA-TOP SECRET facility:

   a. Create a separate Facility Matrix entry for the TAS by renaming an existing entry in the TSS Facility Matrix. You can model this entry after the TSO Facility Matrix entry, except that `NOTSOC` must be specified. The LAS can initialize properly with the standard STC Facility Matrix entry defaults, so a separate facility usually is not needed for the LAS.

      Use the following sample TSSPARM statements to rename an existing entry:

      ```
      FAC(USER8=NAME=BBV)
      FAC(BBVTAS=PGM=BBV,ACTIVE,NOTSOC)
      FAC(BBVTAS=SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF)
      FAC(BBVTAS=LUMSG,STMSG,SIGN(s),INSTDATA)
      FAC(BBVTAS=NORNDPW,AUTHINIT,NOPROMPT,NOAUDIT)
      FAC(BBVTAS=RES,WARNPW,LCFCMD,NOTRACE)
      FAC(BBVTAS=DORMPW,NONPWR,NOIMSXTND,MSGLC)
      FAC(BBVTAS=MODE=FAIL)
      ```

b. After an IPL or TSS restart with the new MAINVIEW Alternate Access Facility Matrix entry in place, define interconnections between this Facility Matrix entry, the BBVTAS started task, and its default STC ACID.

   The following are sample TSS (TSO) commands to define these interconnections:

```
TSS  CREATE(BBVTASA)  NAME('bbvtas stc acid') +
  FAC(STC)  PAS(NOPW,0)  DEPT(department-acid) +
  MASTFAC(BBV)

TSS  ADD(STC)  PROC(BBVTAS)  ACID(BBVTASA)
```

c. If you do not have standard STC Facility Matrix entry defaults, as discussed in Step a on page 315, you must also define the LAS ACID with MASTFAC specifying the new MAINVIEW Alternate Access entry.

   The following are sample TSS (TSO) commands to define these interconnections:

```
TSS  CREATE(BBVLASA)  NAME('bbvlas stc acid') +
  FAC(STC)  PAS(NOPW,0)  DEPT(department-acid) +
  MASTFAC(BBV)

TSS  ADD(STC)  PROC(BBVLAS)  ACID(BBVLASA)
```

2. Add the `BOOLEBBV` resource to the class `IBMFAC`.

   The following is a sample TSS (TSO) command to add a `BOOLEBBV` resource to class `IBMFAC`:

```
TSS  ADDTO(owner-acid)  IBMFAC(BOOLEBBV)
```

3. Permit each ACID to be used with an AutoLogon session to have READ access to resource `IBMFAC(BOOLEBBV)`.

   Use the following sample TSS (TSO) command to permit ACID with READ access:

```
TSS  PERMIT(ACID)  IBMFAC(BOOLEBBV)  ACCESS(READ)
```

Customizing Class TERMINAL Access Authorization for CA-TOP SECRET

For CA-TOP SECRET support of terminal access authorization using the `TERMID=` parameter in the RACROUTE VERIFY parameter list, review the following steps and perform any actions necessary for your installation:

1. Define the terminal ID (VTAM LU name or EXCP terminal address) as a protected resource to CA-TOP SECRET in class `TERMINAL` by using the following sample command:

```
TSS ADDTO(owner-acid) TERMINAL(terminal-id)
```

2. Permit each ACID that can log on from this terminal (LU name or address) using the following sample command:

```
TSS PERMIT(acid) TERMINAL(terminal-id) ACCESS(READ)
```

Customizing Class APPL Access Authorization for CA-TOP SECRET

For CA-TOP SECRET support of MAINVIEW Alternate Access application authorization using the `APPL=` parameter in the RACROUTE VERIFY parameter list and VTAM major node name access authorization, review the following steps and perform any actions necessary for your installation:

1. Define the resource `BBVLOGON` in class `APPL` to CA-TOP SECRET using the following sample command:

   ```
   TSS ADDTO(owner-acid) APPL(BBVLOGON)
   ```

2. If EXCP terminal sessions are to be used with MAINVIEW Alternate Access, also define the resource `BBVEXCP` in class `APPL` to CA-TOP SECRET using the following sample command:

   ```
   TSS ADDTO(owner-acid) APPL(BBVEXCP)
   ```

3. Define a resource to CA-TOP SECRET in class `APPL` for each VTAM major node name to be used with MAINVIEW Alternate Access using the following sample command:

   ```
   TSS ADDTO(owner-acid) APPL(major-node-name)
   ```

4. Permit each ACID that needs to log on to MAINVIEW Alternate Access to have READ access to the `BBVLOGON` resource in class `APPL`.

   For example, you may use the following sample command:

   ```
   TSS PERMIT(acid) APPL(BBVLOGON) ACCESS(READ)
   ```

5. Permit each ACID that needs to log on to MAINVIEW Alternate Access using an EXCP session to have READ access to the `BBVEXCP` resource in class `APPL`.

   For example, you may use the following sample command:

   ```
   TSS PERMIT(acid) APPL(BBVEXCP) ACCESS(READ)
   ```

6. Permit each ACID that needs to log on to MAINVIEW Alternate Access using a VTAM terminal to have READ access to the resource in class APPL whose name matches the major node name to be used by MAINVIEW Alternate Access.

   For example, you may use the following sample command:

   ```
   TSS PERMIT(acid) APPL(major-node-name) ACCESS(READ)
   ```

Part 5. Appendixes, Glossary, and Index

The appendixes provide additional information to help you use MAINVIEW security.

Appendix A. Basic Security Problem Determination 321
Before You Contact Customer Support 321
AutoOPERATOR Advanced Security 323
SYSPROG and AutoOPERATOR 324
MAINVIEW for CICS 325

Appendix B. Default Parameters for Enhanced Security 327
Default Parameter Definitions 327
Manually Creating a Parameter Definition Member 327
Understanding Parameter Definitions 328
Default Class Definitions 337
Changing and Adding Classes. 337
Manually Creating a Class Definition Member 337
Understanding Class Definitions 337
Understanding the NEXT= Parameter 350
Transformation List Values for the INTENT= Parameter 351

Appendix C. Using Product Libraries 353
Parameter Libraries 357
BBPARM. 357
UBBPARM 357
IMS Parameter Library (MAINVIEW for IMS, MAINVIEW for DBCTL, and AutoOPERATOR for IMS Only) 357
Sample Libraries 358
BBSAMP. 358
UBBSAMP 358
Profile Libraries 359
BBPROF 359
SBBPROF 359
User BBPROF 360
Procedure Libraries (AutoOPERATOR Only) 360
BBPROC 360
UBBPROC 360
View, Screen, and View Help Distribution Libraries 361
Site Libraries 361
User Libraries 361
Shared Libraries 362
Library Concatenation. 363
Link Library 363
Product Support Data Sets 363
Image and Journal Logs 364
Product Library Customization Summary 365

Glossary 369

Index 379

Appendix A. Basic Security Problem Determination

Basic security for MAINVIEW products through your ESM is controlled by the presence of control statements in the SYS1.PARMLIB member BBSEC. If you make changes to the BBSEC member, you must complete a warm start for these changes to take effect.

To disable security through your ESM, remove the `TYPE=BBI` statement for the BBI-SS PAS and warm start the BBI-SS PAS.

Refer to Chapter 7, "Activating Basic Security" on page 91, for complete information about the correct syntax required in the BBSEC member.

Before You Contact Customer Support

Check the following items before contacting BMC Software Customer Support for your security-related questions:

1. Check the SYSLOG and the BBI Journal for any messages created during initialization.

   The following message is issued during BBI-SS PAS initialization when security through the SAF interface is in use:

   ```
   SM3209I  SECURITY DEFINITIONS RETRIEVED FROM xxxxxxxx ssid
   ```

   where

   xxxxxxxx Identifies whether security has been turned on from either BBPARM or SYS1.PARMLIB

   ssid Is the name of the BBI-SS PAS that is secured

   Use this message to determine which BBI-SS PAS has had security turned on and where it was turned on from.

2. Check the syntax of the TYPE=BBI statement.

   If the message in Step 1 did not show up in the SYSLOG or the BBI Journal during BBI-SS PAS initialization, the syntax of the TYPE=BBI statement in the BBSEC member may be incorrect.

   Security for MAINVIEW products can be implemented from the following levels:

   a. BBSEC member of SYS1.PARMLIB

   b. BBPARM DD name concatenation (normal searching order is used: the first member found is the first one checked for security)

   If multiple TYPE=BBI statements exist through these three levels (regardless if they occur multiple times within a single level), BBI-SS PAS initialization uses only the first statement where the `SS=ssid` keyword matches the ID of the BBI-SS PAS. The match may be due to use of wildcards (asterisks) in the `SS=ssid` keyword.

3. Check to see if the wrong class (`CLASS=classname`) or prefix (`PREFIX=prefix`) is used.

The SM3209I message issued during BBI-SS PAS initialization indicates which library the TYPE=BBI definitions were taken from.

If you think the incorrect BBSEC member is being used, check for unwanted security calls in SYS1.PARMLIB and BBPARM security levels.

Once you find the member, check it for correct syntax usage. If the `CLASS` or `PREFIX` keywords are not specified correctly, the defaults are used. The defaults are `CLASS=$BOOLE` and `PREFIX=BBM`.

Documentation for these keywords is in Chapter 7, “Activating Basic Security” on page 91.

4. Ensure that the secured resource was refreshed correctly within the ESM after changes were made.

   All changes made to a TS user's security access are dynamic. Therefore, once a TS user's authority to access a resource is changed within the ESM, those changes are in effect for the next attempt to access that resource.

   Security checks are done for each command or service. The RACROUTEs are issued by the address space with the use of a third-party RACROUTE. This allows the security administrator to change a TS-user's authority without needing to restart the BBI-SS PAS. You cannot use the .RESET AUTH command once SAF security is active.

   A TS user attempting to gain access to CSM may have to re-log on after changes are implemented. The security check for CSM is done within the TS address space. Once a TSO user attempts to gain access to CSM and that access is denied, the TSO user must log on again after the security administrator grants access. This can be a re-logon; it does not require you to log off and log on.

5. Check the ESM's audit trail for the resource name and user ID verified.

   Because it is possible for a resource to be protected by multiple profiles when generics are in use, you can enable any tracing or auditing facilities the ESM may provide and check this output to determine the exact resource name and user ID the ESM is verifying.

   Note: The ESM uses the most discrete profile.

6. Check to see if the BBI-SS PAS was restarted after changes were made to the BBSEC member.

   All information pertaining to security is obtained from the BBSEC member during BBI-SS PAS initialization. Issuing the command .RESET AUTH has no effect on security through your ESM. All changes to the BBSEC member become effective after a warm start.

AutoOPERATOR Advanced Security

Check the following items if you encounter security problems with AutoOPERATOR advanced security:

1. Check the SYSLOG or the BBI Journal for any of the following messages created during initialization when any AutoOPERATOR advanced security features are in use:

   ```
   AA3210I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=APPL IN USE
   AA3211I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=CMD IN USE
   AA3212I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=EXEC IN USE
   AA3215I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=ALRT IN USE
   AA3216I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=PARM IN USE
   ```

   Each AutoOPERATOR security feature that is implemented generates a separate message.

2. Check the SYSLOG or the BBI Journal for any of the following messages created during initialization when the AutoOPERATOR advanced security feature CMD is in use:

   ```
   AA3214W  TYPE=AAO FEATURE=CMD SPECIFIED WITH SAF CLASS=DATASET
   AA3211I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=CMD IN USE
   ```

   AA3214W is a warning message that is issued any time you start the BBI-SS PAS with a security class of DATASET. This results in resource names for command transactions to be restricted to only the command. Parameters and keywords are not checked.

   The following table shows an example of commands that can be used and the corresponding resource name that is checked for either CLASS=DATASET or CLASS=$BOOLE:

Command issued	**CLASS=$BOOLE**	**CLASS=DATASET**
#D SLIP=ID01	*prefix.ssid*.AAO.*target*MVSCMD.D.SLIP	*prefix.ssid*AAO.*target*MVSCMD.D
/DIS A	*prefix.ssid*.AAO.*target*IMSCMD.DIS.A	*prefix.ssid*.AAO.*target*IMSCMD.DIS
Note: Commands, parameters, and keywords are truncated at eight characters.		

3. When AutoOPERATOR advanced security features are in use, check to see if the correct resource name is defined to the ESM.

   When either AutoOPERATOR advanced Security Feature CMD or EXEC is in use, the more discrete level of checking overrides basic security checks when the command is issued from the TS command line.

The following example shows commands that can be issued and the corresponding resource name that is checked when either CLASS=DATASET or CLASS=$BOOLE is specified:

Command issued	Without advanced security	With advanced security
#D SLIP=ID01	*pre.ssid*.AAO.*target*.MVSCMD	*pre.ssid*.AAO.*target*.MVSCMD.D.SLIP
/DIS A	*pre.ssid*.AAO.*target*.IMSCMD	*pre.ssid*.AAO.*target*.IMSCMD.DIS.A
%TESTEXEC	*pre.ssid*.AAO.*target*.EXEC	*pre.ssid*.AAO.*target*.EXEC.TESTEXEC
Note: Commands, parameters, and keywords are truncated at eight characters.		

The AutoOPERATOR advanced security feature of CMD does not affect BBI commands or SYSPROG commands issued from the COMMAND line. AutoOPERATOR advanced security for CMD affects only:

- CICS Transactions
- IMS Transactions
- IMS Commands
- MVS Commands

SYSPROG and AutoOPERATOR

Check the following items if you encounter security problems with AutoOPERATOR and SYSPROG:

1. If you are experiencing trouble with SYSPROG commands under AutoOPERATOR, check security definitions for both AutoOPERATOR and SYSPROG; for example:

   a. Check RESAUTH authority.

      The RESAUTH parameter controls all SYSPROG commands issued by the TS.

   b. Check the TS user's authority in SYSPROG.

      If the TS user has RESAUTH authority and the command still fails, check the SYSPROG security definitions.

      Once AutoOPERATOR determines that the TS user has authority to issue a SYSPROG command, that command is passed to SYSPROG for further processing. Authority to issue that particular command is determined by SYSPROG.

MAINVIEW for CICS

Check the following items if you encounter security problems with MAINVIEW for CICS:

1. Check the SYSLOG and the BBI Journal for the following message created during initialization when security through the ESM is in use:

   ```
   BCO006I  SECURITY DEFINITIONS FOR TYPE=CICS IN USE
   ```

   Note: This message might not be contiguous with other security messages issued; there may be intervening messages.

2. Check the syntax of the TYPE=CICS statement.

   If the message in Step 1 did not show up in the SYSLOG or the BBI Journal during BBI-SS PAS initialization, the syntax of the TYPE=CICS statement in the BBSEC member may be incorrect.

   Refer to Chapter 7, “Activating Basic Security” on page 91, for complete information about the correct syntax required in the BBSEC member.

Appendix B. Default Parameters for Enhanced Security

The following sections discuss default security parameters and default class property table parameters.

Default Parameter Definitions

The security parameter definitions for the subsystem are distributed in member BBMTSS as shown in Figure 29 on page 328. These default parameters are in effect in the subsystem until you specify changes to them.

There are two ways to change the default parameters:

- Use the parameter definition views to create a new parameter definition member in the BBSECURE library with a suffix of 00. See Chapter 12, "Parameter Definitions" on page 155, for information about accessing and using these views; see Table 46 on page 329 for information about each parameter.
- Create and edit a member manually. Sometimes you cannot access the parameter definition views because of your ESM configuration, but you need to change the default parameter definitions to disable security resource access authorizations completely, for example. See "Manually Creating a Parameter Definition Member" for instructions on defining a parameter definition member manually.

Manually Creating a Parameter Definition Member

To create and edit a parameter definition member manually:

1. Copy member BBMTSS in the BBACTDEF library for the CAS to a member named BBMTSS00 in the BBSECURE library.

   Warning

   Do not access BBACTDEF member BBMTSS in ISPF edit mode. This action will destroy your security subsystem and render the CAS unavailable. Your product will need to be reinstalled.

2. Edit member BBMTSS00 in the BBSECURE library. Initially, it will contain the statements shown in Figure 29 on page 328. You need to modify only the parameters required by your ESM. Valid parameter values are listed in Table 46 on page 329.

Understanding Parameter Definitions

Figure 29 shows the parameter definitions that ship with your product.

See Table 46 on page 329 for information about each parameter and the different values that can be defined either manually or automatically through the CHANGE SECURITY PARAMETERS dialog.

```
ESM ESMTYPE(AUTO)       /* AUTOMATICALLY DETERMINE ESM TYPE         */
    PRODUCTS(BBI3)      /* BASE PRODUCT                             */
    SUBSYS(SSID)        /* RACROUTE SUBSYS= IS CAS SSID             */
    REQSTOR(ASIS)       /* RACROUTE REQSTOR= REMAINS UNCHANGED      */
    APPL(SSID)          /* RACROUTE APPL= DEFAULT IS CAS SSID       */
    SESSTYPE(NONE)      /* RACROUTE SESSTYPE= IS NOT SPECIFIED      */
    ESMUID(ACCEPT)      /* ESM-DEFINED USERIDS ARE NOT REQUIRED     */
    DFLTUID(NONE)       /* DEFAULT ESM USERID IF ESMUID(ACCEPT)     */
    PGMRNAME(ALLOW)     /* USER CAN SPECIFY PROGRAMMER NAME         */
    ESMGRINH(ALLOW)     /* ALWAYS ALLOW GROUP IDENT INHERITANCE     */
    ACCTINFO(ALLOW)     /* USER CAN SPECIFY ACCOUNTING INFO.        */
    DFLTACCT(EXTERNAL) /* DEFAULT ACCOUNT INFO. DEFINED BY ESM     */
    TSSPRIVPGM(STD)     /* TOP SECRET PRIVILEGED PROGRAM NAME       */
    TSSMSGS(ALL)        /* RETRIEVE TSS MESSAGES FROM FDBK & SAF    */
    ACF2MSGS(ALL)       /* RETRIEVE ACAF2 MESSAGES FROM FDBK & SAF  */
    ENTITYX(YES)        /* ESM SUPPORTS RACROUTE AUTH ENTITYX=      */
    DSTYPE(M)           /* ESM SUPPORTS RACROUTE AUTH DSTYPE=M      */
    TRACE(NONE)         /* SECURITY TRACES NOT INITIALLY ENABLED    */
    RSLIMIT(3)          /* SECURITY SERVER SUBTASK WILL RESTART     */
    RSINTERVAL(60)      /* AUTOMATICALLY UP TO 3 TIMES IN TO MIN    */
    WINMSG(NONSAFE)     /* BYPASS DISPLAY OF "SAFE" SECURITY MSGS   */
    ;
```

Figure 29. Default BBMTSS Parameter Definition Member

Table 46. Parameter Definitions

Description	Parameter
`ESMTYPE=(`*esmtype*`)` (ESM Type field)	Specifies the type of ESM in use on this MVS. The following values may be specified for *esmtype*: AUTO — Attempts to determine automatically which ESM is installed and has been activated. RACF — RACF (IBM Program Product). TSS — CA-TOP SECRET. ACF2 — CA-ACF2. SAF — Generic SAF interface. NONE — No SAF-compatible external security manager. **Important** Specifying `ESMTYPE(NONE)` effectively bypasses security for the entire subsystem. This may be inappropriate for your site. When defined, an uncustomizable, nonbypassable call to the security system is made during CAS initialization using the following parameters: Class name — FACILITY Entity name — BBMSS.ESMTYPE.NONE A RACF profile, a CA-TOP SECRET permit, or a CA-ACF2 rule need not exist to authorize `ESMTYPE(NONE)`, but, if it does, the CAS must be permitted UPDATE or WRITE access thereto.
`PRODUCTS(`*product*`)`	Reserved for future use. Currently, the value specified for the PRODUCT parameter must be BBI3.
`RELEASE(`*release*`)`	Specifies the release level of the ESM in use on this MVS system. Normally, it is not necessary to specify this parameter. The following values may be specified for *release*: 1.9 With RACF or SAF Version 1.9 2.1 With RACF or SAF Version 2.1 2.2 With RACF or SAF Version 2.2 4.2 With CA-TOP SECRET Release 4.2 4.3 With CA-TOP SECRET Release 4.3 4.4 With CA-TOP SECRET Release 4.4 5.0 With CA-TOP SECRET Release 5.0 5.2 With CA-ACF2 Release 5.2 6.0 With CA-ACF2 Release 6.0 6.1 With CA-ACF2 Release 6.1 6.2 With CA-ACF2 Release 6.2 **Note:** If `ESMTYPE(AUTO)` is specified, the `RELEASE` parameter should not be specified.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`SUBSYS(`*subsys*`)` (Subsys ID field)	Specifies the one- to eight-character subsystem name to be passed to the ESM by the `SUBSYS=` parameter of the RACROUTE macro instruction. The following values may be specified for *subsys*: APPL — Current value of the `APPL` parameter. APPLID — Current CAS VTAM application name. JOBNAME — Current CAS JOB name. STEPNAME — Current CAS STEP name. PROCSTEP — Current CAS PROCedure stepname. SSID — MVS subsystem ID defined for use by the CAS. SMFID — Current MVS image SMF identifier. NONE — Nothing. Do not pass a `SUBSYS=` value to RACROUTE. " — Null. No `SUBSYS=` value is passed to the ESM by RACROUTE (same as NONE). '*string*' — Specified one- to eight-character string is passed to the ESM by RACROUTE.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`REQSTOR(`*ctrlpt*`)` (Reqstor field)	Specifies the one- to eight-character requestor or control point name to be passed to the ESM by the `REQSTOR=` parameter of the RACROUTE macro instruction. The following values may be specified for *ctrlpt*: ASIS — Requestor value is not altered from that specified by MAINVIEW itself in the resource definition table entry. APPL — Current value of the `APPL` parameter. APPLID — Current CAS VTAM application name. JOBNAME — Current CAS JOB name. STEPNAME — Current CAS STEP name. PROCSTEP — Current CAS PROCedure stepname. SSID — MVS subsystem ID defined for use by the CAS. SMFID — Current MVS image SMF identifier. NONE — Nothing. Do not pass a `REQSTOR=` value to RACROUTE. " — Null. No `REQSTOR=` value is passed to the ESM by RACROUTE (same as NONE). '*string*' — Specified one- to eight- character string is passed to the ESM by RACROUTE.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`APPL(`*`applid`*`)` (Applid field)	Specifies the one- to eight-character application name to be passed to the ESM by the `APPL=` parameter of the RACROUTE macro instruction. The following values may be specified for *applid*: APPLID — Current CAS VTAM application name. JOBNAME — Current CAS JOB name. STEPNAME — Current CAS STEP name. PROCSTEP — Current CAS PROCedure stepname. SSID — Current CAS address space MVS subsystem ID. SMFID — Current MVS image SMF identifier. NONE — Nothing. Do not validate application access. " — Null. No `APPL=` value is passed to the ESM by RACROUTE (same as NONE). '*string*' — Specified one- to eight-character string is passed to the ESM by RACROUTE.
`SESSTYPE(`*`type`*`)` (Session type field)	Is the session type to be specified to the ESM by RACROUTE `REQUEST=VERIFY,ENVIR=CREATE`. The following values may be specified for *type*: TSO — Specify `SESSION=TSO`. NJEBATCH — Specify `SESSION=NJEBATCH`. NONE — Do not specify `SESSION=`.
`ESMUID(`*`process`*`)` (ESM Userid field)	Identifies the ESM user ID processing to be performed. The following values may be specified for *process*: ACCEPT — An external security manager-defined user ID may be specified, used, defaulted, or inherited (but one is not required). REQUIRED — A valid external security manager-defined user ID must be specified, used, defaulted, or inherited. REJECT — A valid external security manager-defined user ID may not be specified or inherited.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`DFLTUID(`*dfltuid*`)` (Default Userid field)	Is the default user ID to be used if `ESMUID(ACCEPT)` is specified and the user ID provided is not defined to the ESM and no service point-level default user ID has been specified. The following values may be specified for *dfltuid*: NONE — No default user ID has been provided. 'UserID' — Default user ID to be used.
`PGMRNAME(`*value*`)` (Programmer Name)	Indicates whether or not a programmer name field must be passed to the external security manager when a user attempts to sign on. The following values may be specified for *value*: ALLOW — The programmer name specified by the end user, or the default assigned to a user ID, if defined, is passed to the external security manager, but one is not required. IGNORE — A programmer name field is not required and is not passed to the external security manager. REQUIRE — A programmer name field must be provided by the end user.
`ESMGRINH(`*value*`)` (GROUP Inherit field)	Indicates whether or not the inheritance of the GROUP IDENT associated with a user ID's extracted security environment from any originating system to a target system is allowed and, if so, under what circumstances. The following values may be specified for *value*: ALLOW — The GROUP IDENT of a user ID is always inherited, regardless of the inheritance mechanism used to establish a security environment. IGNORE — The GROUP IDENT of a user ID is not inherited. UTKNONLY — The GROUP IDENT of a user ID is inherited only for security environments established by means of a B1 UTOKEN. EXTRONLY — The GROUP IDENT of a user ID is inherited only for security environments established by means of a non-B1 security environment password or ACF2 LOGONID mask extraction. **Important** IBM MVS B1 security guidelines require ALLOW or UTKNONLY to be specified. Any other value for this field is specified at the installation's own risk.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`ACCTINFO(value)` (Accounting information)	Indicates whether or not any session or user ID-related accounting information must be passed to the external security manager. The following values may be specified for *value*: ALLOW — Accounting information is not required and may be blank; if blank, the default value, if specified, will be used. IGNORE — Accounting information is not accepted from the end user, and no accounting information will be passed to the external security manager. REQUIRE — Accounting infomation must be provided by the end user and will be passed to the external security manager.
`DFLTACCT(value)` (Default Account Information)	Indicates the type of default accounting information that is available, if defined. The following values may be specified for *value*: '*value*' — The default accounting information field that will be passed to the external security manager is a quoted variable string value as specified in the Default Account Information field. EXTERNAL — The default accounting information field value specified by the external security manager is to be used. NONE — There is no default accounting information assigned either by the external security manager or externally.
`TSSPRIVPGM(opt)` (TSS Priv Program field)	Is the source of the privileged program name passed to CA-TOP SECRET by the security interface by RACROUTE `REQUEST=FASTAUTH`. The following values may be specified for *opt*: JST — Jobstep task program name is used. STD — Standard privileged program name, BBM9SZ45, is used.
`TSSMSGS(src)` (Display TSS Msgs field)	Is the source of error messages retrieved from CA-TOP SECRET. The following values may be specified for *src*: FBK — TSS feedback area. SAF — Standard SAF interface message return area. ALL — Messages from both areas are merged and processed.
`ACF2MSGS(src)` (Display ACF2 Msgs field)	Is the source of error messages retrieved from CA-ACF2. The following values may be specified for *src*: FBK — CA-ACF2 feedback area (CA-TOP SECRET look-alike). SAF — Standard SAF interface message return area. ALL — Messages from both areas are merged and processed.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`ENTITYX(opt)` (Support EntityX field)	Specifies whether or not the ESM in use supports the RACF 1.9-format `ENTITYX=` parameter format on the RACROUTE `REQUEST=AUTH` macro instruction. The following values may be specified for *opt*: YES `ENTITYX=` is supported. NO `ENTITYX=` is not supported (CA-ACF2 5.2 and earlier, CA-TOP SECRET 4.2 and earlier).
`DSTYPE(x)` (Support DSType=M field)	Specifies whether the ESM in use supports the RACF `DSTYPE=M` parameter on the RACROUTE `REQUEST=AUTH` macro instruction. The following values may be specified for *x*: M Yes, `DSTYPE=M` is supported (VOLSER not needed for `CLASS=DATASET`). N No, `DSTYPE=M` is not supported (must specify `DSTYPE=N`).
`TRACE(trace)` (Security traces field)	The type of security trace messages to be issued to the console. The following values may be specified for *trace*: NONE No security interface activity trace messages are to be issued. SIMPLE Only simple security trace messages are to be issued. EXTENDED Extended security trace messages are to be issued. Simple and Extended Security tracing may be activated and terminated after the CAS has initialized, using the DIAGMSG view.
`RSLIMIT(count)` (Security restart times field)	The restart limit. After this number of automatic security interface server subtask restarts within a period of `RSINTERVAL` minutes, no further automatic restarts are performed. This parameter is used to catch runaway automatic recovery in an ESM abend scenario. A decimal number must be specified for *count*.

Table 46. Parameter Definitions (Continued)

Description	Parameter
`RSINTERVAL(`*`mins`*`)` (Security restart minutes field)	Is the restart interval. After this number of automatic security interface server subtask restarts specified for `RSLIMIT` have occurred within the number of minutes specified for `RSINTERVAL`, no further automatic restarts are performed. This parameter is used to catch runaway automatic recovery in an ESM abend scenario. A decimal number not greater than 1440 must be specified for *mins*
`WINMSG(`*`option`*`)` (Window messages field)	Specifies which security interface-generated and ESM-generated messages are to be displayed in any MAINVIEW window. The following values may be specified for *option*: ALL — All security messages are to be exhibited to the user. NONSAFE — Only *nonsafe* security messages are to be displayed. In other words, *safe* security messages may be bypassed safely and not exhibited to the end user. This reduces the frequency and volume of nuisance security manager and security interface-generated messages.

Default Class Definitions

The default class definitions for the SAF class `FACILITY` are shown in Figure 30 on page 338. These parameters are in effect in the subsystem until you specify changes to these defaults.

Changing and Adding Classes

There are two ways to change and add classes:

- Use the class definition views to add or change default security class parameters in the member with suffix 00 of the security parameter library, as described in Chapter 11, "Class Definitions". See Table 47 on page 339 for information about each class parameter.
- Create a new member or edit a member manually to change the parameters. Sometimes you cannot access the class definition views because of your ESM configuration, but you need to change the default parameters or add new classes. See "Manually Creating a Class Definition Member" on page 337 for instructions on how to define class definitions manually and edit the class definitions.

Manually Creating a Class Definition Member

To create and edit a class definition member manually:

1. Copy member BBMTSP in the BBACTDEF library for the CAS to a member named BBMTSP00 in the security parameter library.

Warning

Do not access BBACTDEF member BBMTSP in ISPF edit mode. This will destroy your security subsystem and render the CAS unavailable. Your product will need to be reinstalled.

2. Edit member BBMTSP00 in the security parameter library. Initially, it will contain definitions for over 70 classes in the statements, as shown in Figure 30 on page 338. You need only modify the parameters required by your ESM. Valid parameter values are listed in Table 47 on page 339.

Understanding Class Definitions

Figure 30 on page 338 shows the class definitions defined for class `FACILITY` and `$BBM` that ship with your product. These two examples are a small sampling of the default class definitions. To see a list of all the default class definitions, display the SECDEF view.

See Table 47 on page 339 for information about each parameter and the different values that can be defined either manually or automatically through the CHANGE SECURITY CLASS DEFINITION or ADD SECURITY CLASS DEFINTION dialogs.

```
FILEDATE                        /*  Most recent update to this member    */
    UPDUSERID = userID          /*  UserID this table updated by         */
    UPDSYSTEM = version         /*  System this table updated on         */
    UPDDATE = date              /*  Date when this table updated         */
    UPDTIME = time              /*  Time when this table updated         */
;
CLASS('$BBM')
    DESCRIPTION = 'BBI-3 Default Resource Class            '
    ACTIVE = YES
    NEXT = 'FACILITY'
    UPDUSERID = JXM1
    UPDSYSTEM = R320
    UPDDATE = 10JAN1995
    UPDTIME = 15:52
;
CLASS('FACILITY')               /*  External Resource CLASS Name         */
    DESCRIPTION = 'IBM or Vendor Defined Miscellaneous Uses'/*           */
    ACTIVE = YES                /*  Resource Class active or not         */
    MAXLEN = 39                 /*  Maximum length of entity name        */
    LOGFAIL = ALLOW             /*  Log Resource Access Failure          */
    LOGAUTH = ALLOW             /*  Log Resource Access Success          */
    INTENT = ( )                /*  Access intent transformations        */
    RESLIST = NO                /*  Build LIST and use FASTAUTH          */
    PREFIX = ''                 /*  Resource Entity Name Prefix          */
    SUFFIX = ''                 /*  Resource Entity Name Suffix          */
    TSSCLASS = UNCHANGED        /*  Top Secret Internal CLASS Name       */
    TSSAUTH = YES               /*  Substitute AUTH for FASTAUTH         */
    TSSFAUTH = NO               /*  Substitute FASTAUTH for AUTH         */
    TSSLIST = OK                /*  Response to LIST build request       */
    TSSDEFPROT = NO             /*  Bypass ownership checking            */
    TSSRESMASK = NO             /*  Extended resource access mask        */
    TSSCLSMASK = NO             /*  Extended class access mask           */
    TSSPRIVPGM = NO             /*  Privileged program name req'd        */
    ACF2RULE = FAC              /*  Generalized Resource Rule Type       */
    ACF2RESDIR = NO             /*  Resource Directory Build req'd       */
    ACF2AUTH = NO               /*  Substitute AUTH for FASTAUTH         */
    ACF2LIST = PERFORM          /*  Response to LIST build request       */
    UPDUSERID = JXM1            /*  UserID this entry updated by         */
    UPDSYSTEM = R320            /*  System this entry updated on         */
    UPDDATE = 27JAN1995         /*  Date when this entry updated         */
    UPDTIME = 14:26             /*  Time when this entry updated         */
```

Figure 30. Partial Default BBMTSP00 Class Definition Member

Table 47. Class Definitions

Parameter	Description
`CLASS('intclass')` (Class Name field)	Specifies the internal class name whose attributes are to be defined. The *'intclass'* value is a one- to eight-character class name referenced by a resource manager. **Note:** Internal class names are fixed and cannot be altered. All possible internal class names to be referenced by the component are already defined in CLASS statements in the distributed member BBMTSP.
`DESCRIPTION = 'description'` (Description field)	Specifies a user-readable description of the class. The parameter value is a string of up to 40 characters that must be delimited with enclosing apostrophes.
`NEXT='nxticlas'` (NextClass field)	Specifies the one- to eight-character class name of the next `CLASS` statement that contains class name and access attribute transformation specifications. These specifications also are to be applied to resource access authorization requests by resource managers using this class name. The `NEXT=` parameter provides benefits in defining and maintaining your class definitions. For more information about the `NEXT=` parameter, see "Understanding the NEXT= Parameter" on page 350.
`ACTIVE = YES|NO` (Active field)	Specifies whether the class is active. The following values may be specified: YES — The class is active, and resource access attribute and entity name transformation (including the `NEXT=` parameter) processing continues normally. NO — The class is considered inactive. Any resource access authorization request that uses this class name (or any request that reaches here through a previous specification of the `NEXT=` parameter) is not passed to the ESM, but instead causes the security interface to respond to the resource manager with return code 04, which indicates that the resource is undefined (or unprotected). **Note:** Interprets return code 04 the same as return code 00.

Table 47. Class Definitions (Continued)

Parameter	Description
`MAXLEN = length` (Max field)	Specifies the maximum length of the resource entity name that is supported by the ESM. The following *length* values may be specified: CDT — Maximum length is determined by the RACF class descriptor table entry for this class name. STD — Maximum length is that implied by CA-TOP SECRET RDT entry attribute STD (nominally, 8). LONG — Maximum length is that implied by CA-TOP SECRET RDT entry attribute LONG (nominally, 44). integer — Maximum length is the integer value specified.
`LOGFAIL = option` (LogFail field)	Specifies whether, in the case of resource access authorization failure, logging by the ESM is to be allowed. The following *option* values may be specified: ALLOW — If specified in the resource profile, logging of access authorization failures is to be permitted. NEVER — If resource access authorization fails, it is not to be logged by the ESM.
`LOGAUTH = option` (LogAuth field)	Specifies whether, in the case of resource access authorization success, logging by the ESM is to be allowed. The following *option* values may be specified: ALLOW — If specified in the resource profile, logging of a successful access authorization is to be permitted. NEVER — If resource access authorization is permitted, it is not to be logged by the ESM.
`INTENT = (list)` (Execute, Read, Update, Control, Alter, Create, Write, and Delete fields)	Specifies a list of access intent transformations (which may be null), separated by commas, to be performed on the resource access authorization. See "Transformation List Values for the INTENT= Parameter" on page 351 for information about acceptable *list* values.

Table 47. Class Definitions (Continued)

Parameter	Description
`RESLIST = option` (Reslist field)	Specifies whether or not resource access authorizations for all requests for this class are to be handled through FASTAUTH. The following *option* values may be specified: YES — If a resource manager requests authorization for a resource in this class without a prior request to build a resource list, a resource list is built and FASTAUTH is used to search the list to authorize all user access thereafter. You should not specify `RESLIST=YES` for any class that you intend to or might expect to change while the CAS is still running, because there is no way to refresh the resource list once it has been built by this method. MAINVIEW normally causes a list to be built and searched through FASTAUTH for none of the standard classes, but the use of this parameter will not normally be required. NO — If a resource manager requests authorization for a resource in this class without a prior request to build a resource list, the request will be passed to the ESM in the normal manner (REQUEST=AUTH) without first building a resource list. Specifying `RESLIST=NO` does not prevent the resource manager from explicitly requesting that a resource list be constructed and subsequently searched through FASTAUTH. However, for classes that normally are not so treated, doing so prevents one from being built automatically by the security interface. **Note:** Normally, it is not necessary for you to specify `RESLIST=YES`, since the resource managers already properly process the standard classes in the manner required for expected full function. The `RESLIST=YES` parameter should be used only under special circumstances and then only at the direction of support personnel. The `RESLIST=YES` parameter is intended for use with CA-TOP SECRET, with classes that require special authorization attributes (such as privileged program name and extended resource or class attribute masks) that are available only when the FASTAUTH interface is used. This parameter also is intended for use with CA-ACF2 under certain circumstances when a global resource directory has **not** been constructed to process generalized resource rules with masking characters in the rule keys.

Table 47. Class Definitions (Continued)

Parameter	Description

`PREFIX = 'prefix'`
 	
(Prefix field)
	Specifies that the entity name is to be prefixed with the string value specified, which must be enclosed in apostrophes. If no prefix is to be applied, specify a null string as the value for the prefix (two consecutive apostrophes).
	
	The prefix is applied even if the `NEXT=` parameter is specified, and the new resource entity name with the specified prefix added is passed to the next resource name/attribute transformation phase as it may specify them. Therefore, all of the `PREFIX=` values are cumulative.
	
	The maximum length of the prefix is subject only to the maximum length of the entity name as supported by the ESM. Normally, however, you should not use a prefix string with a length greater than nine characters (one data set name index level, plus a period delimiter).
	
	For example, to cause all entity names used by ordinary CA-ACF2 data set access rules with initial rule key of $BBM, specify the following commands in member BBMTSP00:
	
	`CLASS('$BBM')  /* Default Resource Class */`
	`  PREFIX='$'  /* Put "$" at the beginning  */`
	`  NEXT='DATASET'  /* of entity name and jump to entry*/`
	`  ;  /* for class 'DATASET' to finish.  */`

`SUFFIX = 'suffix'`
 	
(Suffix field)
	Specifies that the entity name is to be suffixed with the string value specified, which must be enclosed in apostrophes. If no suffix is to be applied, specify a null string as the value for the suffix (two consecutive apostrophes).
	
	The suffix is applied even if the `NEXT=` parameter is specified, and the new resource entity name with the specified suffix added is passed to the next resource name/attribute transformation phase as it may specify them. Therefore, all of `SUFFIX=` values are cumulative.
	
	The maximum length of the suffix is subject only to the maximum length of the entity name as supported by the ESM. Normally, however, you should not use a suffix string with a length greater than nine characters (one data set name index level, plus a period delimiter).
	
	For example, to cause all entity names to use generic RACF data set profiles that follow a convention that has been established for use with other products and that requires some additional suffix on the profile to trigger the generic profile, specify the following commands in member BBMTSP00:
	
	`CLASS('$BBM')  /* Default Resource Class */`
	`  SUFFIX='.BBM'  /* Add ".BBM" to the end of the  */`
	`  NEXT='DATASET'  /*  entity name and jump to entry */`
	`  ;  /*  for class 'DATASET' to finish`

Table 47. Class Definitions (Continued)

Parameter	Description
`TSSCLASS = tss-class` (Class field in TopSecret section)	Specifies the internal class name used when CA-TOP SECRET is the ESM. The following values may be specified: '*tssclass*' One- to eight-character (internal) class name, which must be enclosed in apostrophes, to be passed to TSS for resource authorizations for this (external) class name. UNCHANGED Specifies that no class name transformation is to be performed, and the internal class name as currently specified is to be passed to TSS as the external class name. **Note:** In the SECDEFD view's ADD SECURITY CLASS DEFINITION or CHANGE SECURITY CLASS DEFINITION dialog, *unchanged* is denoted by blanks, or a blank `Class Name` field in the TopSecret section of the dialog. DISALLOW Specifies that this (internal or external) class name is disallowed in a TSS environment, and such requests, if inadvertently made, will be rejected. CA-TOP SECRET requires that the security interface pass the internal TSS class name (rather than the external class name that is used with the TSS command interface) for certain resource access authorizations. All such classes that are normally referenced by any resource manager are already properly defined according to TSS requirements in member BBMTSP. Certain internal class names are supported by TSS for the REQUEST=AUTH or FASTAUTH interfaces for special, very privileged functions that manipulate resources, return information about them, or alter TSS system operation. These classes should never appear in a normal RACROUTE resource access authorization SAF parameter list. To ensure that you do not inadvertently select one of these special, restricted names for a class, member BBMTSP already includes CLASS statements that specify the restricted class names with the specified TSSCLASS=DISALLOW attribute. Normally, you will not have to specify this parameter on any CLASS statement that you add to BBMTSP00, unless you want to disallow specifically any access to what would otherwise be a valid internal or external class name.

Table 47. Class Definitions (Continued)

Parameter	Description
`TSSAUTH = option` (Auth field in TopSecret section)	Specifies whether a standard AUTH request is to be substituted for a FASTAUTH request when CA-TOP SECRET is the ESM. The following values may be specified: YES — If TSS is your ESM, a RACROUTE REQUEST=AUTH is to be performed instead for this class under all circumstances, even when the resource manager requests that a resource list be built and requests resource access authorization through RACROUTE REQUEST=FASTAUTH. NO — AUTH is not substituted for FASTAUTH in a TSS environment. This parameter is intended mainly for use in diagnostic scenarios.
`TSSFAUTH = option` (FastAuth field in TopSecret section)	Specifies whether a special FASTAUTH request is to be substituted for a standard AUTH request when CA-TOP SECRET is the ESM. The following values may be specified: YES — If TSS is the ESM, a RACROUTE REQUEST=FASTAUTH is to be performed instead for this class under all circumstances, even when the resource manager has not requested that a resource list be built and does not request resource access authorization through RACROUTE REQUEST=FASTAUTH. NO — FASTAUTH is not substituted for AUTH in a TSS environment. TSSFAUTH=YES is normally used, together with TSSCLASS='tssclass', to force certain classes to be authorized through FASTAUTH. This is because of special TSS requirements forced onto the security interface to support all TSS PERMIT command language parameters (such as PRIVPGM) that are not supported through AUTH.

Table 47. Class Definitions (Continued)

Parameter	Description
`TSSLIST = response` (List field in TopSecret section)	Specifies the response by the security interface to a request by a resource manager (when running in a CA-TOP SECRET environment) to build a resource list. A resource list is built in anticipation of subsequent FASTAUTH resource access authorization requests. The following values may be specified: OK — Resource list build request is ignored, and a successful return code that indicates that profiles actually exist in the specified class is returned to the resource manager. TSS does not support RACROUTE REQUEST=LIST. If one is executed, no action is taken and a successful return code is always returned to the caller. PERFORM — Resource list build request is to be acted upon normally, as if TSS actually supported the RACROUTE REQUEST=LIST call, and the return code actually returned by TSS is processed as it would be for RACF. NOPROFILES — Resource list build request is ignored, and a successful return code that indicates that no profiles exist in the class is returned to the resource manager. ALREADY — Resource list build request is ignored, and a warning return code that indicates that a resource list for the class has already been built is returned to the resource manager. BADCLASS — Resource list build request is ignored, and an error return code that indicates that the class is invalid is returned to the resource manager.
`TSSDEFPROT = option` (DefProt field in TopSecret section)	Specifies whether resource ownership checking is to be assumed (by way of bypassing checking) in a CA-TOP SECRET environment. The following values may be specified: YES — Resource ownership checking is to be bypassed. NO — Resource ownership checking is to be performed. TSSDEFPROT=YES should be specified only for those internal TSS classes that support it and for which you want resource ownership checking to be bypassed. For more information about bypassing ownership checking, refer to the appropriate CA-TOP SECRET documentation.

Table 47. Class Definitions (Continued)

Parameter	Description
`TSSRESMASK = option` (ResMask field in TopSecret section)	Specifies whether the resource entity name requires an extended resource access mask in the first character that follows the entity name (at offset +8 for MAXLEN=STD; at offset +44 for MAXLEN=LONG) in a CA-TOP SECRET environment. The following values may be specified: YES Extended resource access mask is required. NO Extended resource access mask is not required. For more information about bypassing ownership checking, refer to the appropriate CA-TOP SECRET documentation.
`TSSCLSMASK = option` (ClassMask field in TopSecret section)	Specifies whether the class name requires an extended class access mask in the first character that follows the class name (at offset +8 for all classes) in a CA-TOP SECRET environment. The following values may be specified: YES Extended class access mask is required. NO Extended class access mask is not required. DATASETX is an example of an internal/external TSS class name that requires the extended class access mask value. For more information on bypassing ownership checking, refer to the appropriate CA-TOP SECRET documentation.
`TSSPRIVPGM = option` (PrivPgm field in TopSecret section)	Specifies whether the resource entity name requires a privileged program name in the second through ninth characters that follow the entity name (at offset +9 for MAXLEN=STD; at offset +45 for MAXLEN=LONG) in a CA-TOP SECRET environment. The following values may be specified: YES Privileged program name is required. NO Privileged program name is not required. For more information on bypassing ownership checking, refer to the appropriate CA-TOP SECRET documentation.

Table 47. Class Definitions (Continued)

Parameter	Description
`ACF2RULE = typ` (Rule field in ACF2 section)	Specifies, for CA-ACF2 environments, the underlying three-character generalized resource rule type that corresponds to the SAF class in question, as mapped by the SAFMAPS GSO record. The following values may be specified: NONE — Specifies that this class name does not map to a CA-ACF2 generalized resource rule type. Generally, all class names map to a generalized resource rule type, except DATASET. Classes not used (or not relevant) in the CA-ACF2 environment may be specified to have the ACF2RULE=NONE attribute. typ — Is the three-character CA-ACF2 generalized resource rule type. Generally, most CA-ACF2 rule types may be specified without the enclosing apostrophes. 'typ' — Is the three-character CA-ACF2 generalized resource rule type, enclosed in apostrophes. You must use this form of specification if the three-character rule type, without apostrophes, happens to match a reserved keyword used in the specification of parameters in these members. The security interface can usually determine, from internal CA-ACF2 control blocks, which CA-ACF2 generalized resource rule type, if any, a SAF class has been mapped to (through the SAFMAPS or CLASMAP GSO records). If the security interface cannot determine which rule type is being used, this specification will be used instead. If there is a mismatch, a warning message is issued to alert you, so that it can be corrected. **Note:** You should ensure that the values used for all class names in member BBMTSP are correct, and, if not, respecify them in member BBMTSP00. In many cases, the resource rule types will be different because of customization decisions made by your enterprise.

Table 47. Class Definitions (Continued)

Parameter	Description

`ACF2RESDIR = option`
 	
(Resdir field in ACF2 section)
	Specifies, for CA-ACF2 environments, whether a CA-ACF2 resource rule directory is required to be built for the underlying generalized resource rule type to process resource access authorization requests properly. The following values may be specified:
	
	YES A CA-ACF2 resource directory is required.
	
	NO A CA-ACF2 resource directory is not required.
	
	A CA-ACF2 resource rule directory will be required when all the following are true:
	
	• CA-ACF2 masking characters are used in the resource rule keys.
	• The class is one that is not normally accessed through resource managers and the security interface using the SAF RACROUTE REQUEST=FASTAUTH interface. (For classes that are accessed in that manner, the resource list build request that *is* made will result in the construction of a resource directory in the appropriate address space. No further installation action will be required to process those classes properly.)
	• A resource directory for the underlying generalized resource rule type has not been made globally resident through the INFODIR or RESDIR GSO record.
	
	If you have specified that a resource directory for the underlying generalized resource rule type be made globally resident through INFODIR, it is not necessary to request that one be built in each using address space.
	
	Here is an example of how to specify to CA-ACF2 that rules of type FAC are to be made globally resident. From the TSO READY prompt, type the following commands:
	
	`ACF`
	`SET CONTROL(GSO) SYSID(sysid)`
	`CHANGE INFODIR ADD TYPES(R-RFAC)`
	`END`
	
	Normally, you will not have to specify ACF2RESDIR=YES for any classes accessed through the standard definitions included in the distributed BBMTSP member. This may not still be the case, however, if you have customized these specifications using overrides in member BBMTSP00.

Table 47. Class Definitions (Continued)

Parameter	Description
`ACF2AUTH = option` (Auth field in ACF2 section)	Specifies whether a standard AUTH request is to be substituted for a FASTAUTH request when CA-ACF2 is the ESM. The following values may be specified: YES — If CA-ACF2 is the ESM, a RACROUTE REQUEST=AUTH is to be performed instead for this class under all circumstances, even when the resource manager requests that a resource list be built and requests resource access authorization through RACROUTE REQUEST=FASTAUTH. NO — AUTH is not substituted for FASTAUTH in a CA-ACF2 environment. This parameter is intended mainly for use in diagnostic scenarios.
`ACF2LIST = response` (List field in ACF2 section)	Specifies the response by the security interface to a request by a resource manager (when running in a CA-ACF2 environment) to build a resource list. A resource list is built in anticipation of subsequent FASTAUTH resource access authorization requests. The following values may be specified: OK — Resource list build request is ignored, and a successful return code that indicates that profiles actually exist in the specified class is returned to the resource manager. This value should *not* be specified unless it will *always* be the case that a globally resident directory will be created. **Note:** ACF2 *does* support RACROUTE REQUEST=LIST in a certain manner, for classes normally accessed through RACROUTE REQUEST=FASTAUTH. PERFORM — Resource list build request is to be acted upon normally, and the return code actually returned by CA-ACF2 is to be processed as it would be for RACF. NOPROFILES — Resource list build request is ignored, and a successful return code that indicates that no profiles exist in the class is returned to the resource manager. ALREADY — Resource list build request is ignored, and a warning return code that indicates that a resource list for the class has already been built is returned to the resource manager. BADCLASS — Resource list build request is ignored, and an error return code that indicates that the class is invalid is returned to the resource manager.

Table 47. Class Definitions (Continued)

Parameter	Description
`UPDUSERID = userid`	Specifies, for audit purposes, the UserID (USERID, ACID, LOGONID) of the user who last updated this CLASS statement. You should update this parameter to provide change tracking information.
`UPDSYSTEM = sysid`	Specifies, for audit purposes, the SMF system ID of the MVS image whereon this CLASS statement was last updated. You should update this parameter to provide change tracking information.
`UPDDATE = ddmmmyyyy`	Specifies, for audit purposes, the date (in Gregorian ddmmmyyyy notation) when this CLASS statement was last updated. You should update this parameter to provide change tracking information.
`UPDTIME = hh:mm`	Specifies, for audit purposes, the time (in 24-hour clock hh:mm notation) when this CLASS statement was last updated. You should update this parameter to provide change tracking information.

Understanding the NEXT= Parameter

The purpose of the `NEXT=` parameter is to facilitate cascaded, hierarchical transformations of resource access attributes. This parameter enables multiple internal classes to share one external class (one that is defined to the ESM). This means the initial internal class attribute definitions do not have to be updated simultaneously with duplicate, and otherwise redundant, specifications. Instead, the external class attributes are taken from the final internal class definition, to which all previous internal class definitions map (as specified by the `NEXT=` parameter).

If there is no next `CLASS('nxticlas')` statement defined, *'nxticlas'* becomes the external class name, or the value defined to the current `CLASS` statement, that is passed to the ESM through RACROUTE to process the resource access authorization request.

The final, external class attributes are intended to be taken from the last internal class definition (the one without a `NEXT=` parameter), so, for each `CLASS` statement that specifies the `NEXT=` parameter, only the following (other) parameters on that CLASS statement are effective and actually used to transform the resource access authorization request.

Transformation List Values for the INTENT= Parameter

Each transformation list defined to the `INTENT=` parameter may include the following option:

level1 TO level2
: Specifies that the access intent `level1` is to be transformed to access intent `level2`, as if the resource manager had requested that level of access intent originally. Access intent levels may have the same meaning as corresponding values defined by the administrative command language for each respective ESM, as shown in Table 48.

Table 48. Access Intent Interpretations by the ESM, for a Transformation

Access intent field	**How interpreted by each ESM**			
	IBM RACF	**CA-TOP SECRET**	**CA-ACF2 data set rules access levels**	**CA-ACF2 generalized resource rule service level**
EXECUTE	EXECUTE	FETCH	EXEC	READ
READ	READ	READ	READ	READ
UPDATE	UPDATE	READ plus WRITE	WRITE	UPDATE
WRITE	UPDATE	WRITE	WRITE	UPDATE
CONTROL	CONTROL	WRITE	ALLOC	UPDATE
ALTER	ALTER	ALL	ALLOC	UPDATE
CREATE	ALTER	CREATE	ALLOC	ADD
DELETE	ALTER	SCRTCH	ALLOC	DELETE

level1 RETURNS answer
: Specifies that a resource access request that specifies an access intent of `level1` is not to be passed to the ESM for processing, but will instead cause the security interface to respond to the resource manager with a return code as specified by the ANSWER parameter value. ANSWER parameter values can be specified as follows:

Table 49. Access Intent Interpretations for Level1

Access intent level	**Return code value**
YES	0
MAYBE	4
NO	8

Appendix C. Using Product Libraries

Objective

Of the distributed target libraries, only those libraries and data sets that are changed by customization are described in this section. The purpose of this section is to ensure that site changes to customized product libraries are not lost when your site migrates to a new release or applies product maintenance.

This section provides information about which product libraries to use when you make changes to a product. It explains how the product libraries are created, what their intended use is, and which libraries to use to make your site's changes.

The types of product libraries are as follows:

- SMP-maintained distributed target libraries

  These libraries are created during product installation. They contain load modules, parameters, procedures, samples, views, screen definitions for views, and view help in their original form. The installation procedures are described in the *Product Installation and Maintenance Guide*.

  Note: Never modify these libraries without SMP procedures.

- Site-customized product libraries

  These libraries are created for you by AutoCustomization, or you can create them manually. They contain versions of distributed library members modified to your site's requirements.

- Product-user libraries

  Each user can have their own version of views, screen definitions containing views, and view help in a library with their user ID.

  A user profile (*uprefix.userid.*BBPROF) is created during TS initialization if one does not exist already depending upon what products are installed.

- Image and Journal Logs

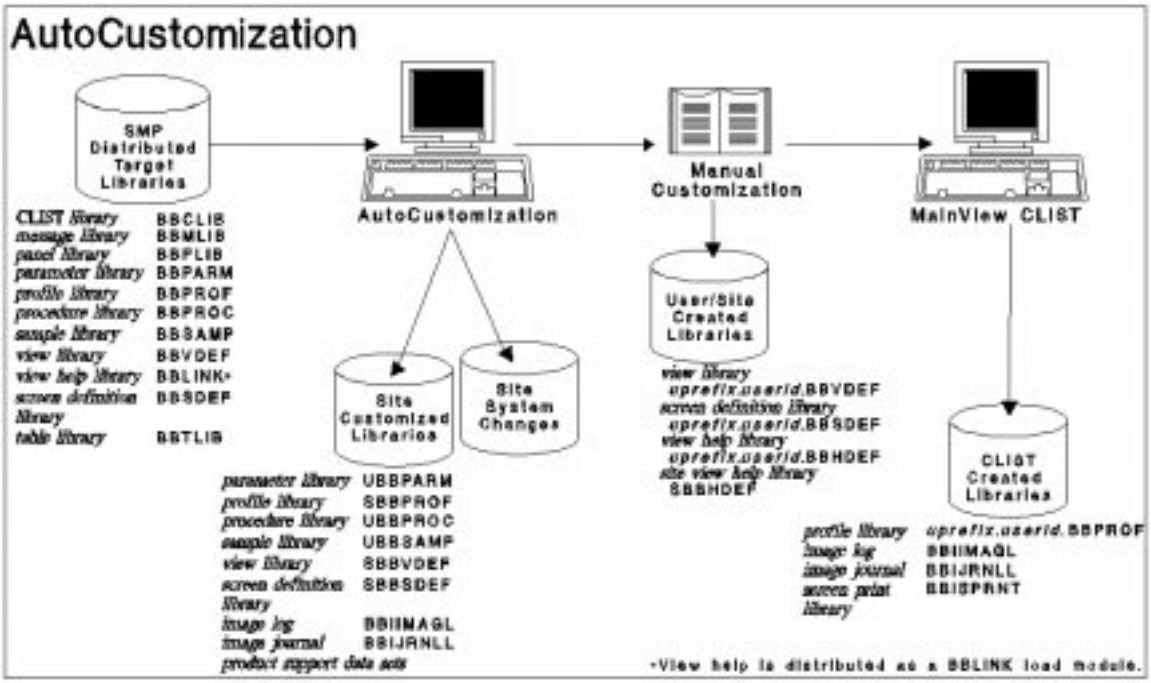
  These logs are used by some products that run in the BBI-SS PAS for recording screen images or messages. They are created for you by AutoCustomization, or you can create them manually.

- Product support data sets

  These data sets are required for some product functions. They are created for you by AutoCustomization, or you can create them manually.

Note: AutoCustomization procedures are described in the *Product Installation and Maintenance Guide*. Manual procedures for creating product libraries are described in the *MAINVIEW Implementation Guide*.

Figure 31 shows how customized product libraries are created.



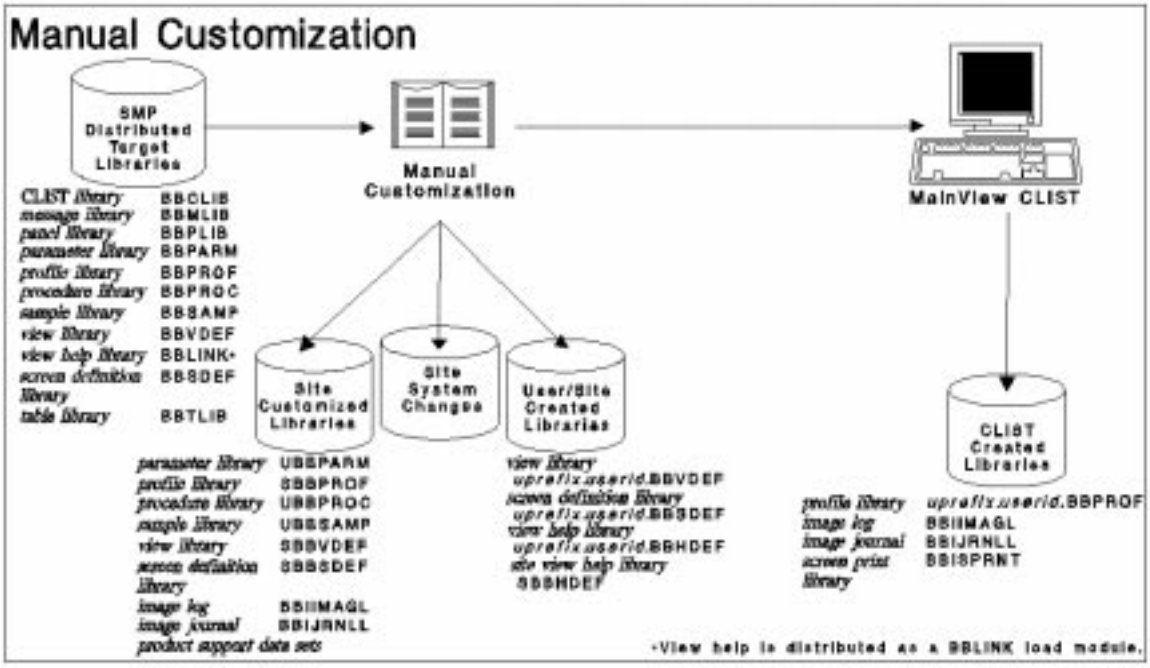


Figure 31. Product Library Customization

Distributed Libraries: The distributed libraries are as follows:

Link library	This data set contains MAINVIEW environment and product-specific load modules.
Parameter library	Product parameters Members in this library contain parameter definitions for related products and product-specific parameter definitions.
Sample library	Product samples Members in this library contain macros, sample JCL, and sample user exit routines.
Profile library	Profile information This library contains members that define PF keys, target system defaults, primary option menu, unique application profiles, and cycle refresh definitions for a user's terminal session for the products that run in full-screen mode.
Procedure library	AutoOPERATOR execute command lists (EXECs) Members in this library contain user-defined automated applications.
View library	Product views Members in this library contain views used by products operating in windows mode.
Screen library	Screen definitions with views Members in this library include screen definintions containing one or more views.
View help library	Help text This library contains help text for products providing views.
Message library	Messages and abend codes This library, called BBMLIB, contains messages and abend codes issued by MAINVIEW products.
Panel library	ISPF panels Each member in this library, called BBPLIB, is a panel definition for the TS. User-customized panels should be placed in a separate library and concatenated in front of the distributed panel library.

CLIST library	MAINVIEW CLISTs AutoCustomization and CLISTs used by specific MAINVIEW products are in this library, called BBCLIB.
Table library	MAINVIEW tables This library, called BBTLIB, contains MAINVIEW product tables, AutoCustomization tables, and some MAINVIEW product command tables.

Note: Use the contents of the distributed libraries as models to create your own site-customized product libraries. The distributed libraries should never be modified. All changes described in this manual should be made only to site-customized product libraries. If you change the distributed libraries, subsequent SMP maintenance will overwrite your changes.

Customized libraries: The customized libraries include some or all of the following:

- Your own versions of the distributed libraries
- Product support data sets

  These are as follows:

  – BBIBBCFG, BBIDIV, BBIVARS

    They are used by all AutoOPERATOR products. BBIBBCFG identifies BBPARM configuration member suffixes to the BBI-SS PAS. BBIDIV is a data storage data set. BBIVARS is a variable pool data set.

  – PARMFILE

    This data set is for MAINVIEW for OS/390 workload configuration definitions and for products supporting historical data processing with the view TIME command.

- Image and Journal Logs

  These are used by the AutoOPERATOR products, MAINVIEW for CICS, MAINVIEW for DB2, MAINVIEW for DBCTL, and MAINVIEW for IMS. The Image log is for screen images from timer-driven service requests. The Journal log is for BBI-SS PAS and product commands, responses, and messages.

Parameter Libraries

Each member in this data set contains parameters for a separate product or group of related products. Your site can have several parameter libraries, a distributed version and one or more site-customized versions. Multiple parameter library data sets can be concatenated together. With this technique, a site parameter library set can be created and a data set individualized for each PAS can be concatenated before the site library.

BBPARM

BBPARM is a distributed target library that is created during product installation. This version should never be modified. Subsequent SMP maintenance will overwrite any changes you make. The distributed name is used in this manual for reference only.

UBBPARM

UBBPARM is a copy of the distributed parameter library. It can be created automatically by AutoCustomization, or you can create it manually.

Note: AutoCustomization creates a UBBPARM data set as *hilevel*.*image*.UBBPARM; for example, *hilevel*.IMAGSYSD.UBBPARM. Using UBBPARM enables each MVS image to have its own BBPARM data set for unique parameters.

Use this copy to make any parameter library changes described in this manual.

AutoCustomization: If you used AutoCustomization successfully when you installed your product libraries as described in the *Product Installation and Maintenance Guide*, it created a UBBPARM data set for you and customized its members.

Manual Customization: If you are customizing the product manually:

1. Create your own UBBPARM data set.
2. Copy the members you need from the distributed BBPARM library into the UBBPARM data set you created.
3. Change the copied members for your needs.

IMS Parameter Library (MAINVIEW for IMS, MAINVIEW for DBCTL, and AutoOPERATOR for IMS Only)

A parameter library, *ibbparm*, where *ibbparm* represents a user-defined parameter library, may be created for each IMS so that each has its own IMFSYS00 member plus any other members that you want to make unique to an IMS target. IMFSYS00 contains BBI-SS PAS to IMS communication parameters. The SUBSYS communication parameter establishes communication between IMS and the BBI-SS PAS.

Manual Customization: A parameter library for a specific IMS must be created manually and copied from the distributed parameter library as described in the customization guides for MAINVIEW for IMS and MAINVIEW for DBCTL. Use this copy of the parameter library to make product changes that are unique to a specific IMS target. For example, different Event Collector initialization parameters can be defined for a specific IMS by copying the

IMFECP00 member from the distributed parameter library to your user-defined parameter library.

Sample Libraries

The members in this data set contain

- sample JCL that can be edited and submitted to perform specified functions
- macros that are referenced when assembling user-written services
- sample user exit routines

Your site can have several sample libraries, a distributed version and one or more site-customized versions. Some members are for more than one product and some are product-specific.

BBSAMP

BBSAMP is a distributed target library that is created during product installation. This version should never be modified. Subsequent SMP maintenance will overwrite any changes you make. The distributed name is used in this manual for reference only.

UBBSAMP

UBBSAMP contains copies of members from the distributed sample library. It can be created automatically by AutoCustomization, or you can create it manually. You can use UBBSAMP to make any changes to members described in this manual.

AutoCustomization: If you used AutoCustomization successfully when you installed your product libraries as described in the *Product Installation and Maintenance Guide*, it created a UBBSAMP data set for you if one did not exist already. UBBSAMP contains copies of members from the distributed sample library. Use these members to customize a product to your site's needs.

Manual Customization: If you are customizing the product manually:

1. Create your own UBBSAMP data set.
2. To change a sample member described in this manual, copy the applicable member or members that you need from the distributed BBSAMP library into the UBBSAMP data set you created.
3. Change the members you copied in UBBSAMP.

Profile Libraries

This section applies only to the following products:

AutoOPERATOR
MAINVIEW for DB2
MAINVIEW for DBCTL
MAINVIEW for CICS
MAINVIEW for IMS

Your site can have several profile libraries, a distributed version and one or more site-customized versions. Members in this data set contain profile information and cycle refresh definitions. Other members are dynamically created. Do not change any members in this library unless instructed to.

You can have a site profile library and a user profile library. The site library can be created automatically by AutoCustomization, or you can create it manually. The site library is a common profile shared by all site users. The MAINVIEW CLIST creates a user profile automatically if one does not exist already. Users should have their own profile library so that each user can specify

- unique PF keys
- CYCLE commands
- target system defaults
- Primary Option Menu
- a unique set of application profiles

The user profile and the site profile should be concatenated before the distributed profile. When a profile is saved, it is stored in the first profile library defined in the concatenation.

BBPROF

BBPROF is a distributed target library that is created during product installation. This version should never be modified. Subsequent SMP maintenance will overwrite any changes you make. The distributed name is used in this manual for reference only.

SBBPROF

SBBPROF is an optional data set. It can be created automatically by AutoCustomization, or you can create it manually. Use SBBPROF to make any changes described in this manual that you want to be shared by all users at your site.

AutoCustomization: If you used AutoCustomization successfully when you installed your product libraries as described in the *Product Installation and Maintenance Guide*, it created an SBBPROF data set for you and customized its members.

Manual Customization: If you are customizing the product manually:

1. Create a common SBBPROF data set for your site.
2. Copy the applicable member or members that you need from the distributed BBPROF library into the SBBPROF data set you created.
3. Change the members you copied in SBBPROF.

User BBPROF

There should be a profile data set for each user so that each user has an individual application profile. The MAINVIEW CLIST created a user profile automatically if one did not exist. It is called *userid.*BBPROF, where *userid* is the user's logon ID. This data set contains profile members customized by a user.

Procedure Libraries (AutoOPERATOR Only)

Your site can have several procedure libraries available, a distributed version and one or more site-customized versions. Members in this data set contain executable procedures used by AutoOPERATOR. These procedures are execute command lists (EXECs) that automate site functions. For more information about EXECs, see the manuals shipped with your AutoOPERATOR product.

BBPROC

BBPROC is a distributed target library that is available when AutoOPERATOR is installed successfully. This version should never be modified. Subsequent SMP maintenance will overwrite any changes you make. The distributed name is used in this manual for reference only.

UBBPROC

UBBPROC is used to contain new user-written EXECs or customized AutoOPERATOR-supplied EXECs from the distributed BBPROC library. It can be created automatically by AutoCustomization or you can create it manually.

AutoCustomization: If you used AutoCustomization successfully when you installed AutoOPERATOR as described in the *Product Installation and Maintenance Guide*, it created a UBBPROC data set for AutoOPERATOR.

If you need to use a specific EXEC sample:

1. Verify that the member was not copied by AutoCustomization to UBBPROC.
2. Copy the sample member you need to modify from the distributed BBPROC to UBBPROC.
3. Make the change in the copied member.

Manual Customization: If you are customizing AutoOPERATOR manually:

1. Create your own UBBPROC data set.
2. Copy the member or members that you need to modify from the distributed procedure library into the UBBPROC data set you created.
3. Change the members you copied in UBBPROC.

View, Screen, and View Help Distribution Libraries

This section applies only to those products operating in windows mode. The distribution libraries for those products are allocated as follows:

Views: The SMP target view library is allocated in the CAS and PAS startup procedure. Site and user view libraries are allocated to the UAS, as described in "Site Libraries" and "User Libraries".

This library contains a uniquely named set of views for a product. View tables allow multiple products to have the same view names. For example, MAINVIEW for OS/390 has one version of VIEWS while CMF MONITOR Online has a completely different version of VIEWS; they are kept separate in the library by being stored in tables with unique names.

Screen definitions: A set of screen definitions is allocated by the MAINVIEW CLIST.

Help text: Help text for views is distributed as a load module in the *hilevel*.BBLINK load library.

Site Libraries

The following site libraries are created for you during AutoCustomization:

- a view library, allocated as *hilevel*.SBBVDEF
- a screen definition library, allocated as *hilevel*.SBBSDEF

The first S in SBBVDEF and SBBSDEF represents "site."

When the MAINVIEW CLIST (created by AutoCustomization) is used to access the MAINVIEW selection menu, *hilevel*.SBBVDEF and *hilevel*.SBBSDEF data sets are allocated to a UAS using the DD names: BBVDEF and BBSDEF.

Note: A system administrator should retain sole authority for adding and deleting views, help text, or screen definitions from site libraries. Granting write authority to more than one user may result in confusion and subject valuable data to overwriting. Users who want to contribute to a site library should contact the system administrator.

If you have an external security system such as RACF, CA-ACF2, or CA-TOP SECRET, it can be used to restrict changes to site libraries from all user IDs except the system administrator's.

User Libraries

User libraries contain customized views, screen definitions, or help text that are available to an individual user only.

Note: If a user does not have access to a user library, any changes made and saved by that user are stored in the site library by default unless the system administrator has prevented write access to the site library. A user library should be created for each user at your site.

1. Create standard partitioned data sets (fixed block, `LRECL=80`) for a user view, screen definition, and help text library.

Use the following naming convention:

uprefix.userid.BB*x*DEF

where

uprefix Is a user's TSO prefix

Note: You can use the UPREFIX parameter in the MAINVIEW CLIST to specify any prefix you want. This is useful for those who have more than one TSO ID and want to use the same user BB*x*DEF data set with all their IDs. If UPREFIX is not specified, the default is *uprefix.userid*.BB*x*DEF.

userid Is a user's TSO ID

x Is one of the following values:

V	View library
S	Screen definition library
H	Help text library

2. Change the user's allocations to contain user and site data sets. Ensure that the user library is searched before the site library.

   Note: If the MAINVIEW CLIST is used to access the MAINVIEW selection menu, it concatenates the view and screen libraries. The user help text library must be added manually to the concatenation.

   As many data sets as needed can be added to the concatenation within your site's restrictions. For example, you may want to create department- or group-specific libraries that only a select group of people may access. All of the people in that department or group, then, would name the same data sets on their BB*x*DEF concatenation.

Shared Libraries

User libraries allocated to a UAS are shared by all products providing views. Therefore, if you have more than one of these products installed on your system, you must use caution when saving views and screen definitions.

For example, suppose you create a MAINVIEW for OS/390 view called MYVIEW and save it in your user view library. You then access CMF MONITOR Online and create another view, also called MYVIEW. When you try to save the second MYVIEW, a message warns you that MYVIEW already exists because you created MAINVIEW for OS/390 MYVIEW previously. If you save the second version anyway, the first version of MYVIEW is overwritten.

To avoid possible confusion, you should establish a naming convention at both the site and user levels; for example, C*xxxxxxx* for CMF MONITOR Online views, M*xxxxxxx* for MAINVIEW for OS/390 views.

Library Concatenation

By default, when views, screen definitions, or help text are changed or new ones created and saved, they are saved in the libraries as follows:

1. User library first, if one exists
2. Site library, if one exists

   If neither one exists, an error message is displayed.

   Note: The distributed view library cannot be overwritten because it is allocated to a PAS, not a UAS.

When views, screen definitions, or help are requested, the libraries are searched by default as follows:

1. Your user library first, if one exists
2. Your site library, if one exists
3. The distributed library (for views and help text only)

Link Library

This data set must be authorized. Executable modules are obtained from this library if it is specified. If it is not specified, an error message is generated. This data set is concatenated in the target's STEPLIB DD statements for some MAINVIEW products.

Product Support Data Sets

AutoOPERATOR products use the following data sets:

- BBIBBCFG

  This BBPARM member specifies which configuration members in the BBPARM library are used when AutoOPERATOR starts. Configuration members control the way AutoOPERATOR works. Default members used are AAOEXP00 and AAOALS00.

- BBIDIV

  This data set is mandatory for AutoOPERATOR. It is used to store binary large objects and data across AutoOPERATOR restarts. It is allocated in the BBI-SS PAS startup procedure.

- BBIVARS

  A profile variable pool. Variables are written to this data set when an EXEC that issues a VPUT ... PROFILE ends or when the VCKP command is issued. It is allocated in the BBI-SS PAS log procedure (BBSAMP member SSLOG).

MAINVIEW for OS/390 and products supporting the DSLIST view and the TIME command use the PARMFILE data set. This VSAM data set is for

- user-defined workload definitions created by the MAINVIEW for OS/390 product

- products providing views of data from a time interval in the past

Data from the past is recorded in historical data sets. PARMFILE is used to contain a directory of the historical data set names, which is shown by a product having a DSLIST view. Data from a historical data set is shown in any of that product's views with the TIME command.

PARMFILE is allocated in the BBI-SS PAS and MVS PAS startup procedures.

Image and Journal Logs

There are two Image and two Journal logs allocated in the BBI-SS PAS startup procedure that are used by the following products:

- AutoOPERATOR (only uses the Journal logs)
- MAINVIEW for MQSeries
- MAINVIEW for CICS
- MAINVIEW for DB2
- MAINVIEW for DBCTL
- MAINVIEW for IMS

The BBI-SS PAS Image log records screen images that are produced automatically by timer-driven analyzer and monitor services. Image logging can be disabled by removing the appropriate statement from the BBI-SS PAS startup procedure.

The BBI-SS PAS Journal log records

- all commands and responses issued from a TS assigned to the BBI-SS PAS
- all commands and responses issued automatically by AutoOPERATOR EXECs
- time stamps for BBI-SS PAS and target system start and stop
- BBI-SS PAS informational, error, and audit messages
- service commands and messages
- DB2 commands and messages

Although it is not recommended, because all operational and diagnostic messages are written to the BBI-SS PAS Journal log, BBI-SS PAS Journal logging can be disabled by removing appropriate DD statements from the BBI-SS PAS startup procedure JCL. BBI-SS PASs cannot share journal data sets.

Note: Image and Journal logs and a screen print data set are allocated to a user's TS by the MAINVIEW CLIST.

Product Library Customization Summary

Table 50 summarizes how the MAINVIEW product libraries should be configured.

Table 50. MAINVIEW Product Library Configuration

Distributed Target Library	Customized Library	Created by AutoCustomization?	Allocated to which Address Space?	Allocated to what DD Name?
BBLINK	BBLINK	No, AutoCustomization APF-authorizes the distributed BBLINK load library and adds it to your system link library. See “Notes” at the end of the table.	UAS, PAS, CICS target, IMS target	BBILOAD or BBILINK
BBSAMP	UBBSAMP	Yes, AutoCustomization creates a UBBSAMP sample library.	None	None
BBPARM	UBBPARM	Yes, AutoCustomization creates a UBBPARM parameter library. See “Notes” at the end of the table.	MVS PAS: BBI-SS PAS, CICS target, IMS target	PARMLIB: BBIPARM
	ibbparm	No, *ibbparm* is a user-defined parameter library that must be created manually.	IMS target	IMFPARM
BBPARM member BBIBBCFG	UBBPARM member CFG*ssid*A	Yes, AutoCustomization creates the UBBPARM member but only for AutoOPERATOR.	BBI-SS PAS	BBCFG
BBPROC	UBBPROC	Yes, AutoCustomization creates a UBBPROC procedure library but only for AutoOPERATOR.	BBI-SS PAS	SYSPROC
None	BBIDIV data set	Yes, AutoCustomization creates this data set but only for AutoOPERATOR.	BBI-SS PAS	BBIDIV
None	BBIVARS data set	Yes, AutoCustomization creates this data set but only for AutoOPERATOR.	BBI-SS PAS	BBIVARS

Table 50. MAINVIEW Product Library Configuration (Continued)

Distributed Target Library	Customized Library	Created by AutoCustomization?	Allocated to which Address Space?	Allocated to what DD Name?
None	BBIIMAG1, BBIIMAG2	Yes, AutoCustomization creates dual Image log data sets for: MAINVIEW for: CICS DB2 DBCTL IMS See “Notes” at the end of the table.	BBI-SS PAS	BBIIMAG1, BBIIMAG2
None	BBIIJRNL1, BBIIJRNL2	Yes, AutoCustomization creates dual Journal log data sets for: AutoOPERATOR MAINVIEW for: CICS DB2 DBCTL IMS MQSeries	BBI-SS PAS	BBIIJRNL1, BBIJRNL2
None	BBIIMAGL, BBIJRNLL	No, AutoCustomization does not create an Image nor a Journal log. They are created automatically by the MAINVIEW CLIST.	UAS	BBIIMAGL BBIJRNLL
BBPROF	*uprefix.userid*.BBPROF and/or SBBPROF	*uprefix.userid*.BBPROF: No, AutoCustomization does not create a user profile. It is created automatically by the TSO MAINVIEW CLIST. SBBPROF: Yes, AutoCustomization creates a site profile.	UAS	BBIPROF

Table 50. MAINVIEW Product Library Configuration (Continued)

Distributed Target Library	Customized Library	Created by AutoCustomization?	Allocated to which Address Space?	Allocated to what DD Name?
BBVDEF	*uprefix.userid*.BBVDEF	No, *uprefix.userid*.BBVDEF is a user-defined view library that must be created manually. The MAINVIEW CLIST allocates it.	UAS	BBVDEF
	hilevel.SBBVDEF	Yes, AutoCustomization creates a *hilevel*.SBBVDEF site view library. The MAINVIEW CLIST allocates it.		
	hilevel.BBVDEF	No, AutoCustomization does not create or modify it. It is a distributed library.	PAS	
BBSDEF	*uprefix.userid*.BBSDEF	No, *uprefix.userid*.BBSDEF is a user-defined screen definition library that must be created manually. The MAINVIEW CLIST allocates it.	UAS	BBSDEF
	hilevel.SBBSDEF	Yes, AutoCustomization creates a *hilevel*.SBBSDEF site screen definition library. The MAINVIEW CLIST allocates it.		
	hilevel.BBSDEF	No, AutoCustomization does not create or modify it. It is a distributed library.		

Table 50. MAINVIEW Product Library Configuration (Continued)

Distributed Target Library	Customized Library	Created by AutoCustomization?	Allocated to which Address Space?	Allocated to what DD Name?
View help text	*uprefix.userid*.BBHDEF	No, *uprefix.userid*.BBHDEF is a user-defined help library that must be created manually. Modify the user's TSO logon procedure to allocate it. See “Notes” below.	UAS	BBHDEF
	hilevel.SBBHDEF	No, AutoCustomization does not create a *hilevel*.SBBHDEF site help library. You must create it manually. The MAINVIEW CLIST allocates it.		

Notes:

- Concatenation

  User and site-customized libraries should be concatenated before the distributed libraries.

- BBLINK

  IMS and CICS target allocation of the link library require IMS and CICS JCL modifications. UAS allocation of the link library uses a DD name of BBILOAD and BBILINK.

- BBPARM

  IMS and CICS target allocation of the parameter library require IMS and CICS JCL modifications.

- View Help text

  Help text for views is distributed as a BBLINK load module.

Glossary

This glossary defines BMC Software terminology. Other dictionaries and glossaries may be used in conjunction with this glossary.

Since this glossary pertains to BMC Software-related products, some of the terms defined may not appear in this book.

To help you find the information you need, this glossary uses the following cross-references:

Contrast with	Indicates a term that has a contrary or contradictory meaning.
See	Indicates an entry that is a synonym or contains expanded information.
See also	Indicates an entry that contains related information.

A

action. Defined operation, such as modifying a MAINVIEW window, that is performed in response to a command. See *object.*

active window. Any MAINVIEW window in which data can be refreshed. See *alternate window, current window, window.*

administrative view. Display from which a product's management tasks are performed, such as the DSLIST view for managing historical data sets. See *view.*

ALT WIN field. Input field that allows you to specify the window identifier for an alternate window where the results of a hyperlink are displayed. See *alternate window.*

Alternate Access. See *MAINVIEW Alternate Access*.

alternate form. View requested through the FORM command that changes the format of a previously displayed view to show related information. See also *form, query.*

alternate window. (1) Window that is specifically selected to display the results of a hyperlink. (2) Window whose identifier is defined to the ALT WIN field. Contrast with *current window.* See *active window, window, ALT WIN field*.

analyzer. (1) Online display that presents a snapshot of status and activity data and indicates problem areas. (2) Component of CMF MONITOR. See *CMF MONITOR Analyzer.*

application. (1) Program that performs a specific set of tasks within a MAINVIEW product. (2) In MAINVIEW VistaPoint, combination of workloads to enable display of their transaction performance data in a single view.

application trace. See *trace.*

ASCH workload. Workload comprising Advanced Program-to-Program Communication (APPC) address spaces.

AutoCustomization. Online facility for customizing the installation of products. AutoCustomization provides an ISPF panel interface that both presents customization steps in sequence and provides current status information about the progress of the installation.

automatic screen update. Usage mode wherein the currently displayed screen is refreshed automatically with new data at an interval you specify. Invoked by the ASU command.

B

batch workload. Workload consisting of address spaces running batch jobs.

BBI. Basic architecture that distributes work between workstations and multiple MVS targets for BMC Software MAINVIEW products.

BBI-SS PAS. See *BBI subsystem product address space.*

BBI subsystem product address space (BBI-SS PAS).

MVS subsystem address space that manages communication between local and remote systems and that contains one or more of the following products:

- MAINVIEW AutoOPERATOR
- MAINVIEW for CICS
- MAINVIEW for DB2
- MAINVIEW for DBCTL
- MAINVIEW for IMS
- Command MQ for S/390
- MAINVIEW VistaPoint (for CICS, DB2, and IMS workloads)

BBPARM. See *parameter library.*

BBPROC. See *procedure library.*

BBPROF. See *profile library.*

BBSAMP. See *sample library.*

BBV. See *MAINVIEW Alternate Access*.

BBXS. BMC Software Subsystem Services. Common set of service routines loaded into common storage and used by several BMC Software MAINVIEW products.

border. Visual indication of the boundaries of a window.

bottleneck analysis. Process of determining which resources have insufficient capacity to provide acceptable service levels and that therefore can cause performance problems.

C

CAS. Coordinating address space. One of the address spaces used by the MAINVIEW windows environment architecture. The CAS supplies common services and enables communication between linked systems. Each MVS image requires a separate CAS. Cross-system communication is established through the CAS using VTAM and XCF communication links.

CFMON. See *coupling facility monitoring.*

chart. Display format for graphical data. See also *graph.*

CICSplex. User-defined set of one or more CICS systems that are controlled and managed as a single functional entity.

CMF MONITOR. Comprehensive Management Facility MONITOR. Product that measures and reports on all critical system resources, such as CPU, channel, and device usage; memory, paging, and swapping activity; and workload performance.

CMF MONITOR Analyzer. Batch component of CMF MONITOR that reads the SMF user and 70 series records created by the CMF MONITOR Extractor and/or the RMF Extractor and formats them into printed system performance reports.

CMF MONITOR Extractor. Component of CMF that collects performance statistics for CMF MONITOR Analyzer, CMF MONITOR Online, MAINVIEW for MVS, and RMF postprocessor. See *CMF MONITOR Analyzer, CMF MONITOR Online, MAINVIEW for MVS*.

CMF MONITOR Online. Component of CMF that uses the MAINVIEW window interface to present data on all address spaces, their use of various system resources, and the delays that each address space incurs while waiting for access to these resources. See *CMF MONITOR, MAINVIEW for MVS.*

CMF Type 79 API. Application programming interface, provided by CMF, that provides access to MAINVIEW SMF-type 79 records.

CMFMON. Component of CMF MONITOR that simplifies online retrieval of information about system hardware and application performance and creates MAINVIEW SMF-type 79 records.

The CMFMON *online facility* can be used to view data in one or more formatted screens.

The CMFMON *write facility* can be used to write collected data as MAINVIEW SMF-type 79 records to an SMF or sequential data set.

CMRDETL. MAINVIEW for CICS data set that stores detail transaction records (type 6E) and abend records (type 6D). Detail records are logged for each successful transaction. Abend records are written when an abend occurs. Both records have the same format when stored on CMRDETL.

CMRSTAT. MAINVIEW for CICS data set that stores both CICS operational statistic records, at 5-minute intervals, and other records, at intervals defined by parameters specified during customization (using CMRSOPT).

column. Vertical component of a view or display, typically containing fields of the same type of information, that varies by the objects associated in each row.

collection interval. Length of time data is collected. See also *delta mode, total mode.*

command delimiter. Special character, usually a **;** (semicolon), used to stack commands typed concurrently on the COMMAND line for sequential execution.

COMMAND line. Line in the control area of the display screen where primary commands can be typed. Contrast with *line command column.*

Command MQ Automation D/S. Command MQ agents, which provide local proactive monitoring for both MQSeries and MSMQ (Microsoft message queue manager). The Command MQ agents operate at the local node level where they continue to perform functions regardless of the availability of the MQM (message queue manager) network. Functionality includes automatic monitoring and restarts of channels, queue managers, queues and command servers. In cases where automated recovery is not possible, the agents transport critical alert information to a central console.

Command MQ Automation S/390. Command MQ component, which monitors the MQM (message queue manager) networks and intercedes to perform corrective actions when problems arise. Solutions include:

- Dead-Letter Queue management
- System Queue Archival
- Service Interval Performance solutions
- Channel Availability

These solutions help ensure immediate relief to some of the most pressing MQM operations and performance problems.

Command MQ for D/S. Command MQ for D/S utilizes a true client/server architecture and employs resident agents to provide configuration, administration, performance monitoring and operations management for the MQM (message queue manager) network.

Command MQ for S/390. Delivers comprehensive capabilities for configuration, administration, performance monitoring and operations management for an entire MQM (message queue manager) network.

COMMON STORAGE MONITOR. Component of MAINVIEW for MVS that monitors usage and reconfigures MVS common storage blocks.

composite workload. Workload made up of a WLM workload or other workloads, which are called *constituent workloads.*

constituent workload. Member of a composite workload. Constituent workloads in a composite usually belong to a single workload class, but sometimes are mixed.

contention. Occurs when there are more requests for service than there are servers available.

context. In a Plex Manager view, field that contains the name of a target or group of targets specified with the CONTEXT command. See *scope, service point, SSI context, target context*.

CONTEXT command. Specifies either a MAINVIEW product and a specific target for that product (see *target context*) or a MAINVIEW product and a name representing one or more targets (see *SSI context*) for that product.

control statement. (1) Statement that interrupts a sequence of instructions and transfers control to another part of the program. (2) Statement that names samplers and other parameters that configure the MAINVIEW components to perform specified functions. (3) In CMF MONITOR, statement in a parameter library member used to identify a sampler in the extractor or a report in the analyzer, or to describe either component's processing requirements to the operating system.

coupling facility monitoring (CFMON). Coupling facility views that monitor the activity of your system's coupling facilities.

CPO. Customized Product Offering. Delivery and installation technique that allows any combination of BMC Software SMP/E-maintainable products to be distributed on a product tape to a customer and installed quickly. The CPO product tape contains libraries required for product customization and execution, plus SMP distribution libraries and data sets needed for application of SMP maintenance.

current data. Data that reflects the system in its current state. The two types of current data are realtime data and interval data. Contrast with *historical data.* See also *interval data and realtime data.*

current window. In the MAINVIEW window environment, window where the main dialog with the application takes place. The current window is used as the default window destination for commands issued on the COMMAND line when no window number is specified. Contrast with *alternate window.* See *active window, window*.

D

DASD. Direct Access Storage Device. (1) A device with rotating recording surfaces that provides immediate access to stored data. (2) Any device that responds to a DASD program.

DASD ADVISOR. An interactive software tool that diagnoses DASD performance problems and makes recommendations to reduce overall service time. This tool measures and reports on the operational performance of IBM and IBM-compatible devices.

data collector. Program that belongs to a MAINVIEW product and that collects data from various sources and stores the data in records used by views. For example, MAINVIEW for MVS data collectors obtain data from MVS services, MVS control blocks, CMF MONITOR Extractor control blocks, and other sources. Contrast with *extractor.*

delta mode. (1) In MAINVIEW for DB2 analyzer displays, difference between the value sampled at the start of the current statistics interval and the value sampled by the current analyzer request. See also *statistics interval.* (2) In CMFMON, usage mode wherein certain columns of data reflect the difference in values between one sample cycle and the next. Invoked by the DELta ON command. See also *collection interval, sample cycle, total mode.*

DMR. See *MAINVIEW for DB2.*

DSO. Data Set Optimizer. CMF MONITOR Extractor component that uses CMF MONITOR Extractor data to produce reports specifying the optimal ordering of data sets on moveable head devices.

E

element. (1) Data component of a data collector record, shown in a view as a field. (2) Internal value of a field in a view, used in product functions.

element help. Online help for a field in a view. The preferred term is *field help.*

Event Collector. Component for MAINVIEW for IMS and MAINVIEW for DBCTL that collects data about events in the IMS environment. This data is required for Workload Monitor and optional for Workload Analyzer (except for the workload trace service). This data also is recorded as transaction records (X'FA') and program records (X'F9') on the IMS system log for later use by the batch products: Performance Reporter and Transaction Accountant. If the Extensions for DB2 option to IMS PR, IMS TA, IMS WA, or IMS WM is installed, the Event Collector also measures DB2 activity through the Attach facility.

expand. Predefined link from one display to a related display. See also *hyperlink.*

Extensions for DB2. Additions to MAINVIEW for IMS and MAINVIEW for DBCTL that gather DB2 subsystem activity through the IMS Attach facility. These additions are licensed as options to IMS PR, IMS TA, IMS WA, and IMS WM. No license is required for IMS RA, IMS RM, and MAINVIEW AutoOPERATOR for IMS.

Extensions for IRLM. Additions to MAINVIEW for IMS and MAINVIEW for DBCTL that analyze database locking and measure IRLM activity when IRLM is used. These additions are licensed as options to IMS RA and IMS RM.

extractor. Program that collects data from various sources and keeps the data control blocks to be written as records. Extractors obtain data from services, control blocks, and other sources. Contrast with *data collector.*

extractor interval. See *collection interval.*

F

fast path. Predefined link between one screen and another. To use the fast path, place the cursor on a single value in a field and press Enter. The resulting screen displays more detailed information about the selected value. See also *hyperlink.*

field. Group of character positions within a screen or report used to type or display specific information.

field help. Online help describing the purpose or contents of a field on a screen. To display field help, place the cursor anywhere in a field and press PF1 (HELP). In some products, field help is accessible from the screen help that is displayed when you press PF1.

filter. Selection criteria used to limit the number of rows displayed in a view. Data that does not meet the selection criteria is not displayed. A filter is composed of an element, an operator, and an operand (a number or character string). Filters can be implemented in view customization, through the PARm/QPARm commands, or through the Where/QWhere commands. Filters are established against elements of data.

fixed field. Field that remains stationary at the left margin of a screen that is scrolled either right or left.

FOCAL POINT. MAINVIEW product that displays a summary of key performance indicators across systems, sites, and applications from a single terminal.

form. One of two constituent parts of a view; the other is query. A form defines how the data is presented; a query identifies the data required for the view. See also *query, view.*

full-screen mode. Display of a MAINVIEW product application or service on the entire screen. There is no window information line. Contrast with *windows mode.*

G

global command. Any MAINVIEW window interface command that can affect all windows in the window area of a MAINVIEW display.

graph. Graphical display of data that you select from a MAINVIEW window environment view. See also *chart.*

H

hilevel. For MAINVIEW products, high-level data set qualifier required by a site's naming conventions.

historical data. (1) Data that reflects the system as it existed at the end of a past recording interval or the duration of several intervals. (2) Any data stored in the historical database and retrieved using the TIME command. Contrast with *current data, interval data and realtime data.*

historical database. Collection of performance data written at the end of each installation-defined recording interval and containing up to 100 VSAM clusters. Data is extracted from the historical database with the TIME command. See *historical data.*

historical data set. In MAINVIEW products that display historical data, VSAM cluster file in which data is recorded at regular intervals.

hyperlink. (1) Preset field in a view or an EXPAND line on a display that permits you to

- Access cursor-sensitive help
- Issue commands
- Link to another view or display

The transfer can be either within a single product or to a related display/view in a different MAINVIEW product. Generally, hyperlinked fields are highlighted. (2) Cursor-activated short path from a topic or term in online help to related information. See also *fast path.*

I

Image log. Collection of screen-display records. Image logs may be created for both the BBI-SS PAS and the BBI terminal session (TS).

The BBI-SS PAS Image log consists of two data sets that are used alternately: as one fills up, the other is used. Logging to the BBI-SS PAS Image log stops when both data sets are filled and the first data set is not processed by the archive program.

The TS Image log is a single data set that wraps around when full.

IMS PERFORMANCE REPORTER (IMS PR). Offline product that organizes data and prints reports that can be used to analyze IMS performance.

IMS PR EXTENSIONS for DB2. Licensed option to the IMS Performance Reporter that provides offline statistical, graphic, and calendar reports about DB2 subsystem activity and requests that are integrated with IMS activity.

IMS RA EXTENSIONS for DB2. Additions to the IMS Resource Analyzer that provide online monitoring displays of DB2 region connection and thread status.

IMS RESOURCE ANALYZER (IMS RA). Online realtime displays used to analyze IMS resources and determine which are affected by specific workload problems.

IMS RESOURCE MONITOR (IMS RM). Online data collection services used to monitor IMS resources and issue warnings when defined utilization thresholds are exceeded.

IMS RM EXTENSIONS for DB2. Additions to the IMS Resource Monitor that provide timer-driven data collection of DB2 region connection and threads.

IMS TA EXTENSIONS for DB2. Licensed option to the IMS Transaction Accountant that provides integrated accounting of IMS and DB2 activity through the IMS Attach Facility.

IMS TRANSACTION ACCOUNTANT (IMS TA). Offline product used to produce cost accounting and user charge-back records and reports.

IMS WA EXTENSIONS for DB2. Licensed option to the IMS Workload Analyzer that provides

- Timer-driven workload wait and trace data collection
- Displays of the transaction active and wait time for DB2 processing events
- Trace of DB2 subsystem activity

  The trace is either summarized by DB2 calls and CPU usage for DB2 processing or detailed to include call start, elapsed times, SQL statement numbers, and return codes.

IMS WORKLOAD ANALYZER (IMS WA). Online data collection and display services used to analyze IMS workloads and determine problem causes.

IMS WM EXTENSIONS for DB2. Licensed option to the IMS Workload Monitor that provides timer-driven data collection of the types and number of calls issued to a DB2 subsystem, DB2 transaction input queue and response time, and average DB2 CPU time per transaction.

IMS WORKLOAD MONITOR (IMS WM). Online data collection services used to monitor IMS workloads and issue warnings when defined thresholds are exceeded.

IMSPlex System Manager (IPSM). Online service that provides Single System Image views of resources and bottlenecks for applications across one or more IMS regions and systems.

interval data. Cumulative data collected during a collection interval. Intervals usually last from 15 to 30 minutes depending on how the recording interval is specified during product customization. Contrast with *historical data.*

Note: If change is made to the workloads, a new interval will be started.

See also *current data and realtime data.*

InTune. Product for improving application program performance. It monitors the program and provides information used to reduce bottlenecks and delays.

IRUF. IMS Resource Utilization File (IRUF). IRUFs can be either detailed (one event, one record) or summarized (more than one event, one record). A detailed IRUF is created by processing the IMS system log through a program called IMFLEDIT. A summarized IRUF is created by processing one or more detailed IRUFs, one or more summarized IRUFs, or a combination of both, through a sort program and the TASCOSTR program. If the Extensions for DB2 option to IMS PR or IMS TA is installed, the IRUF includes data about DB2 calls made through the IMS Attach Facility.

J

job activity view. Report about address space consumption of resources. See *view.*

journal. Special-purpose data set that stores the chronological records of operator and system actions.

Journal log. Collection of messages. Journal logs are created for both the BBI-SS PAS and the BBI terminal session (TS).

The BBI-SS PAS Journal log consists of two data sets that are used alternately: as one fills up, the other is used. Logging to the BBI-SS PAS Journal log stops when both data sets are filled and the first data set is not being processed by the archive program.

The TS Journal log is a single data set that wraps around when full.

L

line command. Command that you type in the line command column in a view or display. Line commands initiate actions that apply to the data displayed in that particular row.

line command column. Command input column on the left side of a view or display. Contrast with *COMMAND line.*

log edit. In the MAINVIEW for IMS and MAINVIEW for DBCTL program named IMFLEDIT, function that extracts transaction (X‘FA’) and program (X‘F9’) records from the IMS system log. IMFLEDIT also extracts certain records that were recorded on the system log by IMS. IMFLEDIT then formats the records into a file called the IMS Resource Utilization File (IRUF).

M

MAINVIEW. BMC Software integrated systems management architecture.

MAINVIEW AutoOPERATOR. Product that uses tools, techniques, and facilities to automate routine operator tasks and provide online performance monitoring, and that achieves high availability through error minimization, improved productivity, and problem prediction and prevention.

MAINVIEW Alarm Manager. Monitor that reads the data elements produced by products in the MAINVIEW window environment and returns SQL-syntactic statements.

MAINVIEW Alternate Access. Enables MAINVIEW products to be used without TSO by providing access through EXCP and VTAM interfaces.

MAINVIEW control area. In the MAINVIEW window environment, first three lines at the top of the view containing the window information line and the COMMAND, SCROLL, CURR WIN, and ALT WIN lines. The control area cannot be customized and is part of the information display. Contrast with *MAINVIEW display area, MAINVIEW window area.*

MAINVIEW Desktop. Version of the MAINVIEW window interface designed to run on OS/2 and Windows workstations.

MAINVIEW display area. See *MAINVIEW window area.*

MAINVIEW Explorer. Product that provides access to MAINVIEW products from a Web browser running under Windows. MAINVIEW Explorer replaces MAINVIEW Desktop.

MAINVIEW for CICS. Product (formerly MV MANAGER for CICS) that provides realtime application performance analysis and monitoring for CICS system management.

MAINVIEW for DB2. Product (formerly MV MANAGER for DB2) that provides realtime and historical application performance analysis and monitoring for DB2 subsystem management.

MAINVIEW for DBCTL. Product (formerly MV MANAGER for DBCTL) that provides realtime application performance analysis and monitoring for DBCTL management.

MAINVIEW for IMS. Product (formerly MV MANAGER for IMS) that provides realtime application performance analysis and monitoring for IMS management.

MAINVIEW for IP. Product that monitors OS/390 mission-critical application performance as it relates to IP stack usage. Collected data includes: connections, response time statistics, application availability, application throughput, and IP configuration.

MAINVIEW for MVS. System management application (formerly MV MANAGER for MVS). Built upon the MAINVIEW window environment architecture, it uses the window interface to provide access to system performance data and other functions necessary in the overall management of an enterprise.

MAINVIEW for OS/390. System management application (formerly MAINVIEW **for MVS (**prior to version 2.5)). Built upon the MAINVIEW window environment architecture, it uses the window interface to provide access to system performance data and other functions necessary in the overall management of an enterprise.

MAINVIEW for UNIX System Services. System management application that allows you to monitor the performance of the Unix System Services from a MAINVIEW window interface.

MAINVIEW for VTAM. Product that displays application performance data by application, transaction ID, and LU name. This collected data includes: connections, response time statistics, application availability, and application throughput.

MAINVIEW for WebSphere. Product that provides Web monitoring and management for applications integrated with IBM's WebSphere Application Server for OS/390.

MAINVIEW Selection Menu. ISPF selection panel that provides access to all MAINVIEW windows-mode and full-screen mode products.

MAINVIEW VistaPoint. Product that provides enterprise-wide views of performance. Application and workload views are available for CICS, DB2, IMS, and MVS. Data is summarized at the level of detail needed; e.g., reports may be for a single target, an MVS image, or an entire enterprise.

MAINVIEW window area. Portion of the information display that is not the control area and in which views are displayed and windows opened. It includes all but the first three lines of the information display. Contrast with *MAINVIEW control area.*

monitor. Online service that measures resources or workloads at user-defined intervals and issues warnings when user-defined thresholds are exceeded.

MV MANAGER for CICS. See *MAINVIEW for CICS.*

MV MANAGER for DB2. See *MAINVIEW for DB2.*

MV MANAGER for DBCTL. See *MAINVIEW for DBCTL.*

MV MANAGER for IMS. See *MAINVIEW for IMS.*

MV MANAGER for MVS. See *MAINVIEW for MVS.*

MVALARM. See *MAINVIEW Alarm Manager.*

MVCICS. See *MAINVIEW for CICS.*

MVDB2. See *MAINVIEW for DB2.*

MVDBC. See *MAINVIEW for DBCTL.*

MVIMS. See *MAINVIEW for IMS.*

MVMQS. See *Command MQ for S/390*

MVMVS. See *MAINVIEW for OS/390.*

MVS product address space (PAS). Address space containing MVS data collectors, including the CMF MONITOR Extractor. Used by MAINVIEW for MVS and CMF MONITOR products. See *PAS.*

MVScope. MAINVIEW for MVS application that traces both CPU usage down to the CSECT level and I/O usage down to the channel program level.

MVVP. See *MAINVIEW VistaPoint.*

MVVTAM. See *MAINVIEW for VTAM.*

N

nested help. Multiple layers of help pop-up windows. Each successive layer is accessed by hyperlinking from the previous layer.

O

object. Anything you can manipulate as a single unit. MAINVIEW objects can be any of the following: product, secondary window, view, row, column, or field.

You can issue an action against an object by issuing a line command in the line command column to the left of the object. See *action.*

OMVS workload. Workload consisting of MVS OpenEdition address spaces.

online help. Help information that is accessible online.

P

parameter library. Data set comprised of members containing parameters for specific MAINVIEW products or a support component. There can be several versions:

- The distributed parameter library, called BBPARM
- A site-specific parameter library or libraries

  These can be

  – A library created by AutoCustomization, called UBBPARM

  – A library created manually, with a unique name

PAS. Product address space. Used by the MAINVIEW products. Contains data collectors and other product functions. See *MVS product address space (PAS), BBI subsystem product address space (BBI-SS PAS).*

performance group workload. MVS/SP-defined collection of address spaces. See *service class workload, workload definition.*

PERFORMANCE MANAGER. MAINVIEW for CICS online service for monitoring and managing current performance of CICS regions.

PERFORMANCE REPORTER. Product component that generates offline batch reports. The following products can generate these reports:

- MAINVIEW for DB2
- MAINVIEW for IMS
- MAINVIEW for CICS

Plex Manager. Product through which cross-system communication, MAINVIEW security, and an SSI context are established and controlled. Plex Manager is shipped with MAINVIEW window environment products as part of the coordinating address space (CAS) and is accessible as a menu option from the MAINVIEW Selection Menu.

pop-up window. Window containing help information that, when active, overlays part of the window area. A pop-up panel is displayed when you issue the HELP command.

PRGP workload. In MVS/SP 5.0 or earlier, or in compatibility mode in MVS/SP 5.1 or later, composite of service classes. MAINVIEW for MVS creates a performance group workload for each performance group defined in the current IEAIPSxx member.

procedure library. Data set comprised of members containing executable procedures used by MAINVIEW AutoOPERATOR. These procedures are execute command lists (EXECs) that automate site functions. There can be several versions:

- The distributed parameter library, called BBPROC
- A site-specific parameter library or libraries

  These can be

  – A library created by AutoCustomization, called UBBPROC

  – A library created manually, with a unique name

The site-created EXECs can be either user-written or customized MAINVIEW AutoOPERATOR-supplied EXECs from BBPROC.

product address space. See *PAS.*

profile library. Data set comprised of members containing profile information and cycle refresh definitions for a terminal session connected to a BBI-SS PAS. Other members are dynamically created by MAINVIEW applications. There can be several versions:

- The distributed profile library, called BBPROF
- A site-specific profile library or libraries

  These can be

  – A library created by AutoCustomization, called SBBPROF

  – A library created manually, with a unique name

The site library is a common profile shared by all site users. The terminal session CLIST creates a user profile automatically if one does not exist; it is called userid.BBPROF, where userid is your logon ID. User profile libraries allow each user to specify unique PF keys, CYCLE commands, target system defaults, a Primary Option Menu, and a unique set of application profiles.

Q

query. One of two constituent parts of a view; the other is form. A query defines the data for a view; a form defines the display format. See also *form, view.*

R

realtime data. Performance data as it exists at the moment of inquiry. Realtime data is recorded during the smallest unit of time for data collection. Contrast with *historical data.* See also *current data and interval data*.

row. (1) Horizontal component of a view or display comprising all the fields pertaining to a single device, address space, user, etc. (2) Horizontal component of a DB2 table consisting of a sequence of values, one for each column of the table.

RxD2. Product that provides access to DB2 from REXX. It provides tools to query the DB2 catalog, issue dynamic SQL, test DB2 applications, analyze EXPLAIN data, generate DDL or DB2 utility JCL, edit DB2 table spaces, perform security administration, and much more.

S

sample cycle. Time between data samples.

For the CMF MONITOR Extractor, this is the time specified in the extractor control statements (usually 1 to 5 seconds).

For realtime data, the cycle is not fixed. Data is sampled each time you press Enter.

sample library. Data set comprised of members each of which contains one of the following:

- Sample JCL that can be edited to perform specific functions
- A macro that is referenced in the assembly of user-written services
- A sample user exit routine

There can be several versions:

- The distributed sample library, called BBSAMP
- A site-specific sample library or libraries

  These can be

  – A library created by AutoCustomization, called UBBSAMP

  – A library created manually, with a unique name

sampler. Program that monitors a specific aspect of system performance. Includes utilization thresholds used by the Exception Monitor. The CMF MONITOR Extractor contains samplers.

SBBPROF. See *profile library.*

scope. Subset of an SSI context. The scope could be all the data for the context or a subset of data within the context. It is user- or site-defined. See *SSI context, target*.

screen definition. Configuration of one or more views that have been stored with the SAVEScr command and assigned a unique name. A screen includes the layout of the windows and the view, context, system, and product active in each window.

selection view. In MAINVIEW products, view displaying a list of available views.

service class workload. MVS- or MAINVIEW for MVS-defined collection of address spaces.

If you are running MVS Workload Manager (WLM) in goal mode, MAINVIEW for MVS creates a service class workload for each service class that you define through WLM definition dialogs.

If you are running MVS 4.3 or earlier, or MVS/SP 5.1 or later with WLM in compatibility mode, MVS creates a performance group workload instead of a service class. See *performance group workload*.

service objective. Workload performance goal, specified in terms of response time for TSO workloads or turnaround time for batch workloads. Performance group workloads can be measured by either objective. Composite workload service objectives consist of user-defined weighting factors assigned to each constituent workload. There are no MVS-related measures of service for started task workloads.

service point. Specification, to MAINVIEW, of the services required to enable a specific product. Services may be actions, selectors, or views. Each target (e.g., CICS, DB2, or IMS,) has its own service point.

The PLEX view lists all the defined service points known to the CAS to which the terminal session is connected.

service request block (SRB). Control block that represents a routine to be dispatched. SRB mode routines generally perform work for the operating system at a high priority. An SRB is similar to a task control block (TCB) in that it identifies a unit of work to the system. See also *task control block.*

service select code. Code entered to invoke analyzers, monitors, and general services. This code is also the name of the individual service.

session. Total period of time an address space has been active. A session begins when monitoring can be performed. If the product address space (PAS) starts after the job, the session starts with the PAS.

SRB. See *service request block.*

single system image (SSI). Feature of the MAINVIEW window environment architecture that allows you to view and perform actions on multiple MVS systems as though they were a single system. The rows of a single tabular view can contain rows from different MVS images.

SpaceView for MVS. Suite of products that assist in all phases of MVS storage management. SpaceView consists of components that perform automation, reporting, trend analysis, and error correction for storage management in MVS.

SSI. See *single system image.*

SSI context. Name created to represent one or more targets for a given product. See *context, target.*

started task workload. Address spaces running jobs that were initiated programmatically.

statistics interval. For MAINVIEW for DB2, cumulative count within a predefined interval (30-minute default set by the DB2STATS parameter in the distributed BBPARM member BBIISP00) for an analyzer service DELTA or RATE display. Specifying the DELTA parameter displays the current value as the difference between the value sampled by the current analyzer request and the value sampled at the start of the current interval. Specifying the RATE parameter displays the current value by minute (DELTA divided by the number of elapsed minutes).

summary view. View created from a tabular view using the Summarize option in view customization. A summary view compresses several rows of data into a single row based on the summarize criteria.

system resource. See *object.*

T

target. Entity monitored by one or more MAINVIEW products, such as an MVS image, IMS or DB2 subsystem, CICS region, or related workloads across systems. See *context, scope, SSI context*.

target context. Single target/product combination. See *context.*

TASCOSTR. MAINVIEW for IMS and MAINVIEW for DBCTL program that summarizes detail and summary IMS Resource Utilization Files (IRUFs) to be used as input to the offline products.

task control block (TCB). Address space-specific control block that represents a unit of work that is dispatched in the address space in which it was created. See also *service request block.*

TCB. See *task control block*.

terminal session (TS). Single point of control for MAINVIEW products, allowing data manipulation and data display and providing other terminal user services for MAINVIEW products. The terminal session runs in a user address space (either a TSO address space or a standalone address space for EXCP/VTAM access).

TDIR. See *trace log directory.*

threshold. Specified value used to determine whether the data in a field meets specific criteria.

TLDS. See *trace log data set.*

total mode. Usage mode in CMFMON wherein certain columns of data reflect the cumulative value between collection intervals. Invoked by the DELta OFF command. See also *collection interval, delta mode.*

trace. (1) Record of a series of events chronologically listed as they occur. (2) Online data collection and display services that track transaction activity through DB2, IMS, or CICS.

trace log data set (TLDS). Single or multiple external VSAM data sets containing summary or detail trace data for later viewing or printing. The trace log(s) can be defined as needed or dynamically allocated by the BBI-SS PAS. Each trace request is assigned its own trace log data set(s).

trace log directory (TDIR). VSAM linear data set containing one entry for each trace log data set. Each entry indicates the date and time of data set creation, the current status of the data set, the trace target, and other related information.

transaction. Specific set of input data that initiates a predefined process or job.

TS. See *terminal session.*

TSO workload. Workload that consists of address spaces running TSO sessions.

U

UAS. See *user address space.*

UBBPARM. See *parameter library*.

UBBPROC. See *procedure library*.

UBBSAMP. See *sample library.*

user address space. Runs a MAINVIEW terminal session (TS) in TSO, VTAM, or EXCP mode.

User BBPROF. See *profile library.*

V

view. Formatted data within a MAINVIEW window, acquired from a product as a result of a view command or action. A view consists of two parts: query and form. See also *form, job activity view, query.*

view definition. Meaning of data that appears online, including source of data, selection criteria for data field inclusion and placement, data format, summarization, context, product, view name, hyperlink fields, and threshold conditions.

view command. Name of a view that you type on the COMMAND line to display that view.

view command stack. Internal stack of up to 10 queries. For each command, the stack contains the filter parameters, sort order, context, product, and timeframe that accompany the view.

view help. Online help describing the purpose of a view. To display view help, place the cursor on the view name on the window information line and press PF1 (HELP).

W

window. Area of the MAINVIEW screen in which views and resources are presented. A window has visible boundaries and can be smaller than or equal in size to the MAINVIEW window area. See *active window, alternate window, current window, MAINVIEW window area.*

window information line. Top border of a window. Shows the window identifier, the name of the view displayed in the window, the system, the scope, the product reflected by the window, and the timeframe for which the data in the window is relevant. See also *window status field.*

window number. Sequential number assigned by MAINVIEW to each window when it is opened. The window number is the second character in the window status field. See also *window status field.*

window status. One-character letter in the window status field that indicates when a window is ready to receive commands, is busy processing commands, is not to be updated, or contains no data. It also indicates when an error has occurred in a window. The window status is the first character in the window status field. See also *window information line, window status field.*

window status field. Field on the window information line that shows the current status and assigned number of the window. See also *window number, window status.*

windows mode. Display of one or more MAINVIEW product views on a screen that can be divided into a maximum of 20 windows. A window information line defines the top border of each window. Contrast with *full-screen mode.*

WLM workload. In goal mode in MVS/SP 5.1 and later, a composite of service classes. MAINVIEW for MVS creates a workload for each WLM workload defined in the active service policy.

workflow. Measure of system activity that indicates how efficiently system resources are serving the jobs in a workload.

workload. (1) Systematic grouping of units of work (e.g., address spaces, CICS transactions, IMS transactions) according to classification criteria established by a system administrator. (2) In MVS, group of service classes within a service definition.

workload activity view. Tracks workload activity as the workload accesses system resources. A workload activity view measures workload activity in terms of resource consumption and how well the workload activity meets its service objectives.

workload definition. Workload created through the WKLIST view. Contains a unique name, a description, an initial status, a current status, and selection criteria by which address spaces are selected for inclusion in the workload. See *Workload Definition Facility.*

Workload Definition Facility. In MAINVIEW for MVS, WKLIST view and its associated dialogs through which workloads are defined and service objectives set.

workload delay view. Tracks workload performance as the workload accesses system resources. A workload delay view measures any delay a workload experiences as it contends for those resources.

workload objectives. Performance goals for a workload, defined in WKLIST. Objectives may include measures of performance such as response times and batch turnaround times.

Index

Symbols

$BOOLE security class, defining 65
* (asterisk) qualifying character 70
+ (plus) qualifying character 70

A

activating basic security 91
active security, viewing 121
adding
  BBSEC to SYS1.PARMLIB 97
  resource class to CA-TOP SECRET 141
  resource class to RACF 133
  security class definition 146
AOALRTDF CLIST 87
AOALRTPE CLIST 87
AOAPPLDF CLIST 87
AOAPPLPE CLIST 87
AOCMDDF CLIST 87
AOCMDPE CLIST 87
AOEXECDF CLIST 87
AOEXECPE CLIST 87
AOPARMDF CLIST 87
AOPARMPE CLIST 87
authorization
  generic 70
  requests
    common resources 175
    types 175
AutoCustomization
  library 356
  parameter library 357
  procedure library 360
  profile library 359
  sample library 358
AutoLogon 305
AutoOPERATOR
  alert-level security 51, 87
  application-level security 44–48, 87
  command-level security 49–50, 87
  customized libraries 356
  EXEC library 360
  EXEC-level security 51, 87
  MAINVIEW SYSPROG Services 24–34
  parameter-level security 52, 87
  securing resources 42–52

B

basic security
  activating 91
  BBI commands 20
  CICS transactions 21
  DB2 commands 22
  DB2 trace 23
  detail application trace 20–21
  displaying parameter data 22
  EXECs 21
  IMS from AutoOPERATOR 22
  Journal log 20
  Rules Processor 21
  securing MVS commands 21
  SQL text 23
  summary application trace 20
  SYSPROG services commands 22
  targets 20
  trace logs 20
  updating parameter data 22
BBACTDEF 115, 327
BBCLIB library 356
BBI
  architecture 4–5
  commands, basic security 20
BBIBBCFG 363
BBIDIV 363
BBIVARS 363
BBKTRNnn 115
BBMLIB
  description 355
BBMTRNnn 115
BBMTSPnn 115, 337
BBMTSS00 message 160
BBMTSSnn 327
BBMZRNnn 115
BBPARM
  considerations 353
BBPLIB
  description 355
BBPROF
  considerations 353
BBSAMP
  considerations 353
BBSDEF 361
BBSEC
  logical parmlib concatenation 97
BBSEC BBPARM member
  activating security for multiple products 92
  adding to SYS1.PARMLIB 97
  creating 91
  disabling security 98
BBSECURE
  BBMTSS member 327
  sharing security parameter definitions 115
BBTLIB
  description 356
BBVDEF 361

C

CA-ACF2
- adding an SAF resource class for 127
- APPL access 311
- configuring 123
- defining PAS and CAS LOGONIDs 124
- defining rules 129
- generalized resource rules 130
- GSO Record Options 124
- MAINVIEW Alternate Access 308
- ordinary CA-ACF2 data set rules 130
- overview 123
- TERMINAL access authority 311
- updating the CA-ACF2 SAFDEF list 126

CAS
- *See* coordinating address space

CA-TOP SECRET
- adding a new SAF resource class 141
- APPL access authority 317
- configuring 138
- controlling access to product resources 143
- defining a new Facility Matrix entry 139
- defining ownership of resources 142
- defining security attributes for started tasks 140
- MAINVIEW Alternate Access 315
- overview 138
- TERMINAL access authority 316

changing
- security class parameters 147

CICS
- action services 35–41
- AutoOPERATOR for CICS 47
- CICSRACF CLIST 88
- diagnostic services 61
- display services 54–60
- transactions, invoking from AutoOPERATOR 21

CICSRACF CLIST 88

class definitions 145

CLIST
- library
  - description 356

CLIST library 85

CLISTs
- AOALRTDF 87
- AOALRTPE 87
- AOAPPLDF 87
- AOAPPLPE 87
- AOCMDDF 87
- AOCMDPE 87
- AOEXECDF 87
- AOEXECPE 87
- AOPARMDF 87
- AOPARMPE 87
- CICSRACF 88
- DB2CMDDF 85, 89
- DB2CMDPE 85
- MIGUSER 85, 86
- RACFDEF 85, 86

CMF MONITOR
- protected resources 193
- views 267

Command MQ for S/390
- *see* MAINVIEW for MQSeries

command syntax notations xvi

common resources
- basic security 19
- enhanced security 175

communication
- between address spaces 5

configuration
- AutoOPERATOR 363
- data sets 353
- product libraries 354

context in default entity name 112

coordinating address space (CAS)
- description 5

creating
- BBSEC member 91
- global security definitions 14
- resource names
  - for AutoOPERATOR 87
  - for CICS 88
  - for MAINVIEW for DB2 89

customization
- *see also* AutoCustomization
- IMS parameter library 357
- procedure library 360
- sample library 358
- summary of 365
- UBBPARM parameter library 357

D

data sets
- configuration 353
- product support 353
- security 115
- site 361
- user 361

DB2
- securing commands 22, 62
- SQL text 23
- trace 23

DB2CMDDF CLIST 85, 89

DB2CMDPE CLIST 85, 89

DCSTAT view, access to 197, 257

default
- access authorization 175
- entity names 111
- security parameters 115

deleting
- security class definitions 147

detail application trace, basic security 20–21

DIAGSESS view, securing 189

DIAGSTOR view 179

DIAGSYS view, securing 190

disabling
- basic security 98

enhanced security 120
distributed libraries
help text 361
screen definition 361
views 361
Dynamic Parameter Manager, AutoOPERATOR 22

E

enhanced security
disabling 120
entity names 111–113
EXCP terminal, securing access through 53
EXECs (AutoOPERATOR)
EXEC Manager access 45
EXEC Testing Facility 45
procedure library 360
securing 21, 51
securing who can schedule 43
Time-Initiated EXEC requests 46
exits
SYSPROG and CSMON service 100

G

generic authorization 70
global security parameter definitions
default parameters 160
GSO Record Options 124

H

help library 355

I

Image log
BBI-SS PAS 364
description 353
IMS parameter library 357
IMS, securing transactions, command, and messaging within AutoOPERATOR 22
InTune 63

J

Journal log
basic security 20
BBI-SS PAS 364
description 353

L

libraries
CLIST 85
CLISTs 356
concatenated 363
configuration 354
distributed target 353
help 355, 361
link 355, 363
message 355
panel 355
parameter 355
procedure 355
product-user 353
profile 355
sample 355
screen definition 355
security parameters 115
shared 362
site 361
creating 361
customized 353
table 356
user 361
view 355, 361
link library 355, 363
logical parmlib concatentation and BBSEC 97

M

MAINVIEW Alarm Manager
protected resources 209
views 275
MAINVIEW Alternate Access
applications security 307
AutoLogon sessions 305
CA-ACF2 308
CA-TOP SECRET 315
RACF 313
securing 305–317
terminal security 306
terminal session 6
MAINVIEW Explorer 6
protected resources 220
views 282
MAINVIEW for CICS
CICSRACF CLIST 88
protected resources 212
securing resources 212
views 276
MAINVIEW for DATA ACCELERATOR Compression
protected resources 215
views 280
MAINVIEW for DB2
CMD 62
DB2 commands 62
DB2CMDDF CLIST 85
DB2CMDPE CLIST 85
protected resources 217
securing resources 217
views 281
MAINVIEW for IMS
protected resources 221
views 283
MAINVIEW for IP
views 288

MAINVIEW for MQSeries
protected resources 226
views 290
MAINVIEW for OS/390
protected resources 193
views 267
MAINVIEW for UNIX System Services
views 293
MAINVIEW for VTAM
views 298
MAINVIEW for WebSphere
views 300
MAINVIEW SYSPROG Services 24–34
views 292
MAINVIEW VistaPoint
protected resources 259
views 297
MAINVIEW, introduction to 3
masks (#, *, +) 70
message library
description 355
migrating resource names 86
MIGUSER CLIST 85, 86
MVS commands, basic security 21

N

naming convention
overview 16
naming convention for resources
for basic security 17
for enhanced security 111

O

online help
distributed 361

P

panel library
description 355
parameter library 115
AutoCustomization 357
description 355
IMS 357
manual customization 357
using 357
PARMFILE 363
PAS
See product address space
password utility 101
PERMIT syntax
denying access 70
granting access 69
Plex Manager
description 5
protected resources 183
views 266
procedure library
AutoCustomization 360
description 355
manual customization 360
using 360
product address space (PAS)
description 5
product libraries
configuration 354, 365
site-customized 353
types 353
profile library
AutoCustomization 359
description 355
user 353
using 359
profile variable pool 363

R

RACF 132
adding resource classes to 133
APPL access authority 314
basic security 13
controlling access to product resources 136
creating profiles for security 135
MAINVIEW Alternate Access 313
TERMINAL access authority 314
RACFDEF 86
RACFDEF CLIST 85
recovering a deleted security class 152
REDEFINE syntax
enhanced security 136
for MAINVIEW products 66
for RESOLVE PLUS services 68
resource names, creating
for AutoOPERATOR 87
for CICS 88
for MAINVIEW for DB2 89
resource naming convention
for basic security 17
for enhanced security 111
resources
CMF MONITOR 193
common MAINVIEW 175
MAINVIEW Alarm Manager 209
MAINVIEW Explorer 220
MAINVIEW for CICS 212
MAINVIEW for DATA ACCELERATOR Compression 215
MAINVIEW for DB2 217
MAINVIEW for IMS 221
MAINVIEW for IP 225
MAINVIEW for MQSeries 226
MAINVIEW for OS/390 193
MAINVIEW for UNIX Systems Services 255
MAINVIEW for VTAM 261
MAINVIEW for WebSphere 263
MAINVIEW SYSPROG Services 251

MAINVIEW VistaPoint 259
Plex Manager 183
Rules Processor, access to 21

S

sample library
AutoCustomization 358
description 355
manual customization 358
using 358
SBBPROF
considerations 353
SBBSDEF screen library 361
SBBVDEF view library 361
screen definition library 355, 361
security
administrative members 115
BBMTSPnn 337
BBMTSSnn 327
administrative views
SEPDEFL 156
basic 19
CICS action services 35–41
class definition
default parameters 147
CMF MONITOR 193
common resources, ehanced security 175
defining
to CA-ACF2 123
to CA-TOP SECRET 138
to RACF 132
disabling basic 98
disabling enhanced 120
interface 173
introduction 14
MAINVIEW Alarm Manager resources 209
MAINVIEW Alternate Access 305–317
MAINVIEW Explorer resources 220
MAINVIEW FOCAL POINT 63
MAINVIEW for CICS 54–60
MAINVIEW for CICS resources 212
MAINVIEW for DATA ACCELERATOR Compression resources 215
MAINVIEW for DB2 62
MAINVIEW for DB2 resources 217
MAINVIEW for DBCTL 63
MAINVIEW for IMS 63
MAINVIEW for IP 225
MAINVIEW for MQSeries resources 226
MAINVIEW for OS/390 193
MAINVIEW for UNIX Systems Services 255
MAINVIEW for VTAM 261
MAINVIEW for WebSphere 263
MAINVIEW SYSPROG Services 24–34, 251
planning 15–16
Plex Manager resources 183
resource classes
deleting 152
resource names 175
viewing active 121
security class
defining $BOOLE 65
generics 70
security class definition
recovering deleted 152
security parameter library
sharing global security parameter definitions 115
SEPDEFL 156
site libraries
descriptions 353
summary application trace, basic security 20
syntax for REDEFINE
enhanced security 136
MAINVIEW products 66
RESOLVE PLUS services 68
syntax notation xvi
SYSPROG command, access to 194, 200, 256
SYSPROG services, access via AutoOPERATOR 22

T

table library 356
TapeSHARE for AutoOPERATOR 22, 48
target
accessing BBI 20
libraries 353
terminal security, MAINVIEW Alternate Access 306
terminal session
description 6
UAS 6
terminal session (TS) 3
trace log, basic security 20
TS
See terminal session
TYPE statement in BBSEC member 92

U

UACC keyword 66
UAS
See user address space
UBBPARM
considerations 353
parameter library 357
UBBSAMP
considerations 353
parameter library 358
UNDeleting a security class 152
universal access (UACC keyword) 66
UNIX resources 255
user
profile 353
user address space (UAS)
description 6
user exit routines
SYSPROG and CSMON service 100

V

view help library 355
view libraries 361
views
    BBVDEF 361
    DCSTAT 197, 257
    DIAGSESS 189
    DIAGSYS 190
    distributed libraries 361
    library containing product 355
    SBBVDEF library 361

Notes

100035388

BMC Software, Inc., Confidential and Proprietary Information