MainView Security Guide

Supporting

Version 6.0 of MainView Infrastructure
MainView products

November 2010
Contacting BMC Software

You can access the BMC Software website at http://www.bmc.com. From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address          BMC SOFTWARE INC
                 2101 CITYWEST BLVD
                 HOUSTON TX 77042-2827
                 USA

Telephone        713 918 8800 or 800 841 2031

Fax              713 918 8000

Outside United States and Canada

Telephone        (01) 713 918 8800

Fax              (01) 713 918 8000


BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

CICS, DB2, IBM, IMS, MQSeries, MVS, OS/390, RACF, VTAM, WebSphere, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is the registered trademark of Linus Torvalds.

UNIX is the registered trademark of The Open Group in the US and other countries.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

Restricted rights legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC SOFTWARE INC, 2101 CITYWEST BLVD, HOUSTON TX 77042-2827, USA. Any contract notices should be sent to this address.
Customer support

You can obtain technical support by using the BMC Software Customer Support website or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, see “Before contacting BMC.”

Support website

You can obtain technical support from BMC 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this website, you can

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

Support by telephone or e-mail

In the United States and Canada, if you need technical support and do not have access to the web, call 800 537 1813 or send an e-mail message to customer_support@bmc.com. (In the subject line, enter SupID:<yourSupportContractID>, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC

Have the following information available so that Customer Support can begin working on your issue 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 other maintenance level such as PUT or PTF
  - system hardware configuration
  - serial numbers
  - related software (database, application, and communication) including type, version, and service pack or maintenance level
- sequence of events leading to the issue
- 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
License key and password information

If you have questions about your license key or password, contact BMC as follows:

- **(USA or Canada)** Contact the Order Services Password Team at 800 841 2031, or send an e-mail message to ContractsPasswordAdministration@bmc.com.
- **(Europe, the Middle East, and Africa)** Fax your questions to EMEA Contracts Administration at +31 20 354 8702, or send an e-mail message to password@bmc.com.
- **(Asia-Pacific)** Contact your BMC sales representative or your local BMC office.
## Contents

### About this book

- Related publications ........................................... 12
- Conventions ................................................... 13

### Chapter 1  How MainView security works

- Security for windows mode .................................... 16
- Security for full-screen mode .................................. 19
- Security for your products ..................................... 19

### Chapter 2  How to set up your ESM for windows mode

- Security Access requirements ................................... 22
  - MainView common registry requirements .................... 22
  - MainView Alarm Management requirements .................. 22
  - Superuser authority requirements ............................. 22
- Setting up RACF ................................................ 23
- Setting up CA ACF2 ............................................ 25
- Setting up CA Top Secret ...................................... 30

### Chapter 3  What MainView needs to know

- Defining the security parameters ............................... 36
  - For windows mode .......................................... 36
  - For full-screen mode ....................................... 41
- Identifying the security class .................................... 45
  - For windows mode .......................................... 45
  - For full-screen mode ....................................... 49
- Identifying the resources to be secured ....................... 51
  - For windows mode .......................................... 51
  - For full-screen mode ....................................... 57
- Disabling security ................................................ 60
  - For windows mode .......................................... 60
  - For full-screen mode ....................................... 62

### Chapter 4  How to control access to resources

- Controlling access to the CAS .................................. 64
  - Globally securing all CASs .................................. 65
  - Securing individual CASs .................................... 65
- Controlling access to PASs and target systems .................. 66
Controlling access to product data .................................................... 67
  In windows mode ................................................................. 68
  In full-screen mode ............................................................. 70
Controlling access to product actions .......................................................... 71
  In windows mode ................................................................. 72
  In full-screen mode ............................................................. 73
Controlling MainView Alternate Access .......................................................... 75
Controlling access to security resources .......................................................... 78
  For windows mode ................................................................. 78
  For full-screen mode ............................................................. 79

Chapter 5  Troubleshooting security problems 81
  Troubleshooting in windows mode .................................................... 82
    Determining which security members are active .................................. 82
    Using Plex Manager security tracing options .................................... 86
  Troubleshooting in full-screen mode ................................................... 87
    Verifying the status of full-screen security ...................................... 88
    Checking MainView AutoOPERATOR advanced security ...................... 89
    Checking MainView for CICS security ......................................... 91
  Troubleshooting in MainView Explorer .............................................. 92

Appendix A  Case study: MainView for DB2 93
  Windows-mode security ............................................................. 93
  Full-screen mode security ......................................................... 96

Index 99
Figures

MainView Selection Menu .................................................. 17
EZPLEX menu ................................................................. 17
EZSEC menu ................................................................. 18
Sample CA Top Secret USER facility statements ...................... 31
SEPDEFL view ............................................................... 37
Change Global Security Parameters dialog ............................ 38
Sample BBSEC member .................................................... 44
SECDEFL view .............................................................. 46
SECDEF view ............................................................... 46
Change Security Class Definition dialog ................................. 47
SERDEFL view ............................................................... 54
SERDEFOV view ............................................................ 55
Change Security Resource Definition dialog ........................... 56
CASDEFD view, CAS security suffixes ................................. 83
CASDEFD view, PAS security suffix ................................... 84
TGTDEFD view, resource definition member suffix .................. 85
DIAGMSG view .............................................................. 86
Sample Extended Authorization Simple Trace messages .............. 87
Sample CA ACF2 rules for MainView for DB2, windows mode .......... 94
Sample CA ACF2 rules for MainView for DB2, full-screen mode ....... 97
Tables

Types of security that are used by MainView products ........................................ 19
Product IDs for resource entity names in windows mode ................................. 52
Suffixes for resource entity names in windows mode ....................................... 53
Default resource entity definitions for products in windows mode ................. 53
Plex Manager security resources to protect ....................................................... 78
About this book

This book contains information about MainView security and is intended for security administrators or system administrators who are responsible for controlling access to MainView resources. The book is designed to be a primer on MainView security. It covers the security-related tasks that are most commonly performed in the MainView environment.

**NOTE**

For a complete reference of information about the MainView security interfaces and the resource names that are used by various MainView products, refer to the *MainView Security Reference Manual*.

To use this book you should be familiar with the following items:

- your external security manager (ESM)
- the MainView products that are installed at your site

Like most BMC documentation, this book is available in printed and online formats. To request printed books or to view online books and notices (such as release notes and technical bulletins), see the Customer Support website at [http://www.bmc.com/support_home](http://www.bmc.com/support_home). Most product shipments also include the books on a documentation CD.

**NOTE**

Online books are formatted as PDF or HTML files. To view, print, or copy PDF books, use the free Adobe Reader from Adobe Systems. If your product installation does not install the reader, you can obtain the reader at [http://www.adobe.com](http://www.adobe.com).

The software also offers online Help. To access Help, press F1 within any product or click the **Help** button in graphical user interfaces (GUIs).
Related publications

The following related publications supplement this book and the online Help:

<table>
<thead>
<tr>
<th>Category</th>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>installation documents</td>
<td><strong>MainView Installation Guide</strong></td>
<td>provides information about the installation of MainView products on IBM z/OS&lt;sup&gt;®&lt;/sup&gt; systems</td>
</tr>
<tr>
<td></td>
<td><strong>Installation Checklist Generator (ICG)</strong></td>
<td>creates a customized checklist of installation steps and information about installation requirements such as software, storage, and system requirements for your combination of products</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Best Practices: Installation, Implementation, and Maintenance</strong></td>
<td>provides recommendations for the installation, implementation, and maintenance of MainView products</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Common Customization Guide</strong></td>
<td>provides instructions for manually customizing the MainView environment for your products</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Security Reference Manual</strong></td>
<td>provides complete information about the MainView security interfaces for windows mode, full-screen mode, and MainView Alternate Access</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Runtime Component System Configuration and Administration Guide</strong></td>
<td>provides information about configuring and administering the Runtime Component System (RTCS)</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Alternate Access Implementation and User Guide</strong></td>
<td>explains how to configure, start, and stop IBM VTAM&lt;sup&gt;®&lt;/sup&gt; and EXCP AutoLogon sessions to access MainView products without TSO communication support</td>
</tr>
<tr>
<td>core documents</td>
<td><strong>MainView Administration Guide</strong></td>
<td>provides information about MainView operations, targets, single system image contexts, data sets, and diagnostic facilities</td>
</tr>
<tr>
<td></td>
<td><strong>MainView User Guide</strong></td>
<td>provides information about working with MainView products in windows mode, in full-screen mode, and from MainView Explorer</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Alarm Management Guide</strong></td>
<td>explains how to create and install alarm definitions that indicate when exceptions occur in a sysplex</td>
</tr>
<tr>
<td></td>
<td><strong>MainView Reference Summary</strong></td>
<td>provides a summary of commands that can be used to navigate and manage the MainView environment</td>
</tr>
<tr>
<td>notices</td>
<td>release notes, flashes, and technical bulletins</td>
<td>provide important product information and last-minute information</td>
</tr>
</tbody>
</table>
Conventions

This book uses the following special conventions:

- All syntax, operating system terms, and literal examples are presented in this typeface.

- Variable text in path names, system messages, or syntax is displayed in italic text:

  \texttt{testsys/instance/fileName}

- The symbol $=>$ connects items in a menu sequence. For example, \texttt{Actions $=>$ Create Test} instructs you to choose the Create Test command from the Actions menu.

\textbf{NOTE}

MainView messages are documented in the Messages and Codes online display, which you can access by typing \texttt{MSG} on the \texttt{COMMAND} line of any MainView display.
How MainView security works

The MainView environment provides an interface to ESMs (such as IBM RACF®, CA Top Secret, or CA ACF2) by using standard System Authorization Facility (SAF) calls. Two types of security are available for MainView products, depending on the product interface:

- windows-mode security
- full-screen mode security

**Note**
Additional security is available for MainView Alternate Access, which provides access to products through VTAM and EXCP interfaces without TSO communication support. Security for MainView Alternate Access is independent of other product security. If your site uses MainView Alternate Access, see “Controlling MainView Alternate Access” on page 75.

This chapter presents the following topics:

Security for windows mode ......................................................... 16
Security for full-screen mode ..................................................... 19
Security for your products ......................................................... 19
Security for windows mode

MainView products that operate in windows mode can display one or more windows of product data on your screen at a time. The security interface for windows mode

- uses the standard SAF interface to communicate with your ESM
- requires that you define resources to your ESM and grant or deny access to them
- supports user-defined resource name, resource group, and security class definitions
- stores its security definition members in the BBSECURE parameter library, which is read during coordinating address space (CAS) and product address space (PAS) initialization
- fulfills the requirements for United States Department of Defense B1 security
- can be administered online by using MainView security views and dialogs

A good starting point for administering MainView windows-mode security online is the Plex Manager EZSEC menu. To start a MainView TSO session and display the EZSEC menu, perform the following tasks:

1. Display the MainView Selection Menu by executing the MainView CLIST in one of the following ways:

   - Select the appropriate ISPF menu or panel option.
   - On the COMMAND line, issue the following TSO command to execute the MainView CLIST:

     ```tsocmd
     TSO EX 'hilevel.UBBSAMP(MAINVIEW)'
     ```
   - Start a VTAM or EXCP MainView Alternate Access terminal session that executes the MainView CLIST.

The MainView Selection Menu is displayed, as shown in Figure 1 on page 17.
2 Select Plex Manager by typing P in the OPTION field and pressing Enter.

The EZPLEX menu is displayed, as shown in Figure 2.

--- Target Activity ---
- Sum by Area
- Sum by Product
- Sum by System/Product
  Not Summarized

--- SSI Context Activity ---
- Sum by Context
- Sum by Product
  Not Summarized

--- MAINVIEW Logger ---
  Message Log
  Alarm Management

> EZALARMS
3 On the EZPLEX menu, position your cursor on >Security and press Enter.

The EZSEC menu is displayed, as shown in Figure 3.

Figure 3   EZSEC menu

The EZSEC menu contains hyperlinks to other security views, including

| SECDEFL    | list of security class definition members |
| SEPDEFL    | list of security parameter definition members |
| SERDEFL    | list of security resource definition members |

**NOTE**

From anywhere within Plex Manager, you can type EZSEC on the COMMAND line and press Enter to display the EZSEC menu.
Security for full-screen mode

MainView products that operate in full-screen mode display a single product application or service on your entire screen. The security interface for full-screen mode

- uses standard SAF RACROUTE AUTH calls to communicate with your ESM
- requires that you define resources to your ESM and grant or deny access to them
- provides static resources and limited customization of the resource name and security class
- is administered outside of MainView by using a member called BBSEC, which can reside in any of the following places:
  - SYS1.PARMLIB
  - logical PARMLIB concatenation
  - BBIPARM concatenation for a PAS

Security for your products

The type of security that you implement depends on what MainView products you have installed at your site:

- Products that operate only in windows mode (such as MainView for z/OS) use only windows-mode security.
- Products that operate only in full-screen mode (such as MainView FOCAL POINT) use only full-screen mode security.
- Products that operate in both full-screen and windows mode (such as MainView for DB2®) use both types of security.

Table 1 identifies the type of security that is used by each MainView product based on its product interface.

Table 1  Types of security that are used by MainView products (part 1 of 2)

<table>
<thead>
<tr>
<th>Product</th>
<th>Windows mode</th>
<th>Full-screen mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMF MONITOR</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView AutoOPERATOR (including MainView Total Object Manager)</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Table 1  Types of security that are used by MainView products (part 2 of 2)

<table>
<thead>
<tr>
<th>Product</th>
<th>Windows mode</th>
<th>Full-screen mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>MainView FOCAL POINT</td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>MainView for CICS®</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>MainView for DATA ACCELERATOR Compression</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for DB2</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>MainView for DBCTL</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>MainView for IMS Online</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>MainView for IP</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for Linux® – Servers</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for z/OS</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for UNIX® System Services (USS)</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for VTAM</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for WebSphere® Application Server</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView for WebSphere MQ&lt;sup&gt;a&lt;/sup&gt;</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>MainView Infrastructure</td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>- MainView Alarm Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- MainView Explorer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Plex Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MainView Storage Resource Manager (SRM)</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>MainView SYSPROG Services and COMMON STORAGE MONITOR</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>MainView VistaPoint</td>
<td>+</td>
<td></td>
</tr>
</tbody>
</table>

<sup>a</sup> You can also use the IBM WebSphere MQ queue manager to secure the MQ resources that are managed by MainView for WebSphere MQ. For more information, see the MainView for WebSphere MQ User Guide.
How to set up your ESM for windows mode

NOTE
This chapter applies to products that run (either in whole or in part) in windows mode. These are additional procedures that are required to prepare your ESM for use with MainView security in windows mode.

For products that run in full-screen mode, preparing your ESM involves identifying the security class and the resources to be secured. For more information about these procedures, see Chapter 3, “What MainView needs to know.”

This chapter provides instructions for customizing the RACF, CA ACF2, and CA Top Secret ESMs for use with MainView security in windows mode.

This chapter presents procedures for completing the following tasks:

- Setting up RACF .......................................................... 23
- Setting up CA ACF2 ...................................................... 25
- Setting up CA Top Secret ............................................. 30
Security Access requirements

This section discusses security requirements for products that run in windows mode.

MainView common registry requirements

The CAS and PASs need update access to the MainView common registry. The MainView common registry is an HFS or zFS directory structure whose top level is defined to the CAS through the HFSPATH view. For more information on using the HFSPATH view, see the MainView Administration Guide.

MainView Alarm Management requirements

MainView Alarm Management requires security authorization for the following functions:

- displaying MainView product alerts
- processing alarm definitions that launch MainView AutoOPERATOR EXECs

Superuser authority requirements

The following superuser authority requirements exist:

- An OMVS segment that is defined for a CAS must specify UID(0) to grant the CAS superuser authority.

- BMC Discovery for z/OS requires superuser authority.

- MainView for UNIX System Services requires superuser authority.

- The MainView SRM Started Task (SVOS) requires an OMVS segment and The Open Group UNIX superuser authority for the line command HFU. For more information about OMVS segments, see the MainView Administration Guide.

- The MainView for IP PAS requires superuser authority or a RACF resource in the SERVAUTH class as follows:

  IST.NETMGMT.sysname.SNAMGMT

  where sysname is the name of the MVS system on which the PAS is running.
Setting up RACF

If RACF is your primary ESM, you must perform the following procedures to support the MainView security interface:

- Authorize the CAS and PAS started tasks.
- Add a SAF resource class (optional).

For complete information about administering RACF, refer to your RACF documentation.

**To authorize the CAS and PAS started tasks**

1. Define user IDs for the CAS and PAS by using RACF commands, such as

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

2. **NOTE**

To access UNIX System Services data, the MainView for UNIX System Services PAS must have superuser authority. The PAS requires that a user ID be defined to the security system (such as RACF) and assigned to the PAS STC by the security system's facilities.

For RACF, this means updating either the RACF started procedure table (ICHRIN03) or the STARTED class definition. The user ID that is assigned must have an OMVS segment with a home directory of `/` and one of the following UID assignments:

- UID=0 specifically assigned (superuser authority)
- A non-zero UID assigned, but the user ID permitted READ access to security resource `BPX.SUPERUSER` in class FACILITY

The PAS will then switch to an effective UID of 0 at startup.

2. Define the CAS and PAS started tasks.

The following RACF commands show how to associate the user IDs that were defined in step 1 with a specific started task procedure name. In this example, the procedure names 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
```
To add a SAF resource class (optional)

**NOTE**

- If you are using the resource CLASS name FACILITY, you can skip this step.
- If you want to specify a resource CLASS name other than FACILITY (as described in “Identifying the security class” on page 45), you must add the SAF resource CLASS name to the RACF class descriptor table (ICHRRCDE) and the RACF router table (ICHRFR01).

1. Define the new resource CLASS name in the RACF dynamic class descriptor table (CDT), by issuing the following command:

   ```
   RDEFINE CDT class                                      -
   CDTINFO( MAXLENGTH(64) DEFAULTUACC(NONE) -
            FIRST(ALPHA)  CASE(UPPER) -
            OTHER(ALPHA,NUMERIC,NATIONAL,SPECIAL) -
            POSIT(301) RAclist(REQUIRED) -
            GENERIC(ALLOWED) GENLIST(ALLOWED) -
            OPERATIONS(YES) -
            ) UACC(NONE)
   ```

   In the command:

   - BMC suggests MAXLENGTH(64). The required minimum length is 39. Some product resource names, however, are longer when using certain options.

   - BMC suggests CASE(UPPER). Some products generate resource ENTITY names with lowercase characters. If you monitor subsystems that have resources and objects defined in mixed case, you should specify CASE(ASIS).

   - The value used for the POSIT() parameter must be selected appropriately for each MVS system and RACF data base.

2. Activate the dynamic CDT (if it is not already active) or refresh the CDT by using one of the following commands:

   ```
   SETROPTS CLASSACT(CDT) RAclist(CDT)
   ```

   ```
   SETROPTS RAclist(CDT) REFRESH
   ```

3. Activate a new resource class by issuing the following RACF commands for each resource class name:

   ```
   SETROPTS GENERIC(class) GENcmd(class)
   ```

   ```
   SETROPTS CLASSACT(class) RAclist(class)
   ```
Setting up CA ACF2

If CA ACF2 is your primary ESM, you must perform the following procedures to support the MainView security interface:

- Customize Generalized System Options (GSO) record options.
- Authorize the CAS and PAS started tasks.
- Update the SAFDEF list.
- Update the authorized command processor table.
- Add a SAF resource class (optional).

For complete information about administering CA ACF2, refer to your CA ACF2 documentation.

To customize GSO record options

1. Set the GSO record options that are required by MainView security by issuing the following TSO commands:

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

   where

   STC enables started tasks to build security control block structures that support the multi-user address space (MUSASS) environment
   MUSASS enables an address space to secure multiple, discrete entities (such as multiple users logging on to MainView products).
   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 system image.

2. Activate the required options by issuing the following system MODIFY commands:

   F ACF2, REFRESH(OPTS)
   F ACF2, REFRESH(PSWD)
To authorize the CAS and PAS started tasks

1 Define LOGONIDs for the CAS and PAS started tasks by using TSO commands, such as

ACF
SET LID
INSERT USING(ACFSTCID) BBMCAS AME(CAS)+
STC SOURCE(STCINRDR) NOTSO+
MUSASS
INSERT USING(ACFSTCID) BBMPAS NAME(PAS)+
STC SOURCE(STCINRDR) NOTSO+
MUSASS
END

**NOTE**
The following restrictions apply to LOGONIDs for the CAS and PAS:

- The LOGONID must be able to execute as a started task and must be authorized to access all data sets that are used within the address space.
- The MUSASS attribute is required.
- To access UNIX System Services data, the MainView for UNIX System Services PAS requires that a user ID be defined to the security system (such as CA ACF2) and assigned to the PAS STC by the security system’s facilities.

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

A LOGONID can be associated with an address space by

- having an exact match between the started task name and the LOGONID
- using the CA ACF2 started task control installation exit (STCXIT) to establish correspondence between the started task and its associated LOGONID

For information about the STCXIT installation exit, refer to your CA ACF2 documentation.

To update the SAFDEF list

**NOTE**
The MainView security interface passes control point identification information to CA-ACF2 by using the SUBSYS and REQSTOR parameters of the RACROUTE macro instruction. The CA ACF2 SAFDEF list must be updated with information about the control points where RACROUTE calls are being made.
1. Review the SUBSYS security parameter (which is your CAS subsystem ID) by displaying either
   - the SEPDEF view
   - the BBMTSS00 parameter definition member

2. Specify the subsystem ID in a SAFDEF record by using TSO commands, such as

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

   In this example, the subsystem ID for the CAS is BBCS.

3. Refresh the in-storage copy of the SAFDEF list by issuing the following system MODIFY command:

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

**To update the authorized command processor table**

---

**NOTE**

This procedure might have already been performed at your site. Updating the command authorization table is an optional step in MainView customization, as described in the MainView Common Customization Guide.

Ensure that the following programs and commands are specified in the authorized command processor table:

- AOEXEC
- BALCMMSG
- BBM3API
- BBM9TC21
- BBM9TC22
- BBM9TC24
- BBVJSETP
- EMTMPW
- SMLOAD
- TSLOAD
To add a SAF resource class *(optional)*

**NOTE**

- If you are using the security class name FACILITY, you can skip this step.
- If you want to specify a security class other than FACILITY (as described in “Identifying the security class” on page 45), you must define the generalized resource rule type to be used for that SAF resource class.

1. Select the generalized resource rule types to be used in defining the rules to control access to product resources.

2. Update the CLASMAP records by using TSO commands, such as

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

3. Refresh the in-storage copy of the CLASMAP tables by issuing the following system MODIFY command:

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

4. *(optional)* To make the rules for the selected resource rule types resident, perform the following tasks:

   A. Add the resource rule types to the INFODIR GSO record by using TSO commands, such as

      ```
      ACF
      SET CONTROL(GSO)
      CHANGE INFODIR ADD TYPES(R-Rtype)
      END
      ```

   B. Refresh the in-storage INFODIR data by issuing the following system MODIFY command:

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

   C. Rebuild the in-storage directory for a resource rule type by issuing the following system MODIFY command:

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

MainView security does not support nonresident rules with masked rule keys for CAS and Plex Manager resources. If your product-referenced rules are not globally resident, you must direct CA ACF2 to do one of the following tasks:

- build a globally resident rule directory (as described in step 4 on page 28)
- build a directory and bring the rules into private storage (LSQA) when required

You can accomplish this task by specifying YES in

- the **ACF2 Resdir** field of the SECDEF view
- the **ACF2RESDIR** parameter of your security class definition in member BBMTSP00
Setting up CA Top Secret

If CA Top Secret is your primary ESM, you must perform the following procedures to support the MainView security interface:

- Define a Facility Matrix entry for MainView security processing.
- Authorize the CAS and PAS started tasks.
- Add a SAF resource class (optional).
- Define ownership of resources.

For complete information about administering CA Top Secret, refer to your CA-Top Secret documentation.

**NOTE**

To access UNIX System Services data, the MainView for UNIX System Services PAS must have superuser authority. The PAS requires that a user ID be defined to the security system (such as CA Top Secret) and assigned to the PAS STC by the security system’s facilities.

**To define a Facility Matrix entry**

1. Select one of the unused, predefined USER facilities that are provided by CA-Top Secret.

2. Specify the required security attributes in the TSSPARMS data set where the selected USER facility is configured.

*Figure 4 on page 31* illustrates the required statements. In these statements, the names USER9 and RTCS are used as examples.
To authorize the CAS and PAS started tasks

1 Define ACIDs for the CAS and each PAS and associate them with the Facility Matrix entry that was defined for MainView products.

A To define an ACID for the CAS, issue the following TSS CREATE command:

```
TSS CREATE(BBMCAS) NAME('SYSA CAS') +
FACILITY(STC,BBI3) +
PASSWORD(NOPW,0) DEPT(deptacid) MASTFAC(BBI3)
```

In this example, BBMCAS is the ACID that is being defined for the CAS on SYSA. The name of the previously defined Facility Matrix entry is BBI3.

B To define an ACID for a PAS, issue the following TSS CREATE command:

```
TSS CREATE(BBMPAS) NAME('SYSA PAS') +
FACILITY(STC,BBI3) PASSWORD(NOPW,0) +
DEPT(deptacid) MASTFAC(BBI3)
```
2 Define the CAS and PAS as started tasks to CA Top Secret.

A To define the CAS procedure as a started task, issue the following TSS ADDTO command:

TSS ADDTO(STC) PROC(BBICAS) ACID(BBMCAS)

In this example, the CAS procedure called BBICAS is to use the previously defined ACID of BBMCAS.

B To define a PAS procedure as a started task, issue the following TSS ADDTO command:

TSS ADDTO(STC) PROC(BBIPAS) ACID(BBMPAS)

To authorize users to the MainView facility

When users connect to a CAS or PAS, they must be authorized to the same facility as the MASTFAC that is associated with the ACID of the CAS or PAS. The following TSS ADDTO command illustrates the authorization that is needed for each user:

TSS ADDTO(user_ID) FACILITY(BBI3)

In this example, BBI3 is the name of the Facility Matrix entry that was identified as the MASTFAC for the ACID of the CAS and PAS.

To avoid having to authorize each user’s ACID, you could add the BBI3 facility to a department, division, or profile ACID, or even to ALL, as shown here:

TSS ADDTO(ALL) FACILITY(BBI3)

To add a SAF resource class (optional)

**NOTE**

- If you are using the security class name FACILITY, you can skip this step. FACILITY is transformed internally by CA Top Secret to IBMFAC.

- If you want to specify a security class other than FACILITY (as described in “Identifying the security class” on page 45), you must update the CA Top Secret resource definition table (RDT) record.

Update the RDT by issuing the following TSS ADDTO command:

TSS ADDTO(RDT) RESCLASS(class)+ RESCODE(3B) ATTR(PRIVPGM, LONG, GENERIC) + ACLST(NONE, READ, UPDATE, ALL)+ DEFACC(NONE)
where \textit{class} is a user-defined class name to be used by MainView security.

\textbf{NOTE}

- The RESCODE value shown here, X'3B', is only an example. You must choose a two-digit hexadecimal resource code that
  - is within the range permitted by CA Top Secret
  - does not conflict with any other user-defined resource class that has been added to the RDT
- The LONG and GENERIC attributes are required.
- The access levels that are shown (NONE, READ, UPDATE, ALL), and the default access level (NONE) are only examples. You can choose your own access level names and default access level.

\textbf{To define ownership of resources}

To define ownership of the MainView resource name prefix to CA Top Secret, issue the following TSS ADDTO command:

\texttt{TSS ADDTO(ownacid) class(BBM)}

where

\begin{itemize}
  \item \textit{ownacid} is the CA Top Secret organizational ACID record
  \item \textit{class} is the name of the SAF resource class that you are using for MainView resources
  \item If you are using resource class FACILITY, specify the external name, IBMFAC.
  \item \textit{BBM} is the high-level prefix of the MainView resource names that are to be owned in the specified resource class
\end{itemize}
What MainView needs to know

The MainView security interface needs to know about your ESM, the security class that it uses, and the resources that you want to secure. In addition, if you want to disable security completely, MainView needs to know that.

This chapter presents procedures for completing the following tasks:

Defining the security parameters ................................................................. 36
  For windows mode .............................................................................. 36
  For full-screen mode ................................................................. 41
Identifying the security class ............................................................... 45
  For windows mode .............................................................................. 45
  For full-screen mode ................................................................. 49
Identifying the resources to be secured .................................................. 51
  For windows mode .............................................................................. 51
  For full-screen mode ................................................................. 57
Disabling security ...................................................................................... 60
  For windows mode .............................................................................. 60
  For full-screen mode ................................................................. 62
Defining the security parameters

Use the procedures in this section to define or modify the security parameters for your ESM.

For windows mode

**NOTE**

In most cases, MainView security for windows mode can determine which ESM is in use at your site without any input from you. You do *not* need to modify the security parameters unless one of the following conditions exists:

- You use an ESM other than RACF, CA Top Secret, or CA ACF2, such as one that was developed in-house.
- You have both CA ACF2 and RACF installed at your site, but you want to use RACF. You must tell MainView to use RACF because CA ACF2 is installed in such a way that it appears to be the preferred ESM.
- You use the RACF GROUP feature and do not want it to be inherited on a connected system. You must specify IGNORE in the GROUP Inherit field on the Change Global Security Parameters dialog (or the ESMGRINH statement of member BBMTSS00).

If it is necessary to modify the security parameters for products that run in windows mode, you can either

- use the SEPDEF views
- modify member BBMTSS00 directly (as described on page 39)

**To use the SEPDEF views**

1. From within Plex Manager, perform one of the following actions:

   - Use the EZSEC menu:
     1. On the COMMAND line, type **EZSEC** and press Enter.
     - On the COMMAND line, type **SEPDEFL** and press Enter.

   The SEPDEFL view is displayed, as shown in Figure 5 on page 37.
SEPDEFL is a list of parameter definition members. The default member is BBMTSS00 and it appears on SEPDEFL with a member suffix of 00.

2 In the CMD line command field, type S next to member suffix 00 and press Enter.

The SEPDEF view is displayed with the default security parameters that are contained in member BBMTSS00.

### NOTE

The first time the SEPDEFL view is displayed, the **Description** field contains the following message:

Empty member--Select to create

When you select an empty member, the following message appears in the SEPDEF view:

BBMYA819E The parameter member BBMTSS00 is missing

Disregard the message and press Enter to display the default security parameters.

3 On the COMMAND line, type EDIT and press Enter to request an edit session.

4 On the COMMAND line, type CHAnge and press Enter.

The Change Global Security Parameters dialog is displayed, as shown in Figure 6 on page 38.
For information about the fields on this dialog, press the Help key.

5 To identify a specific ESM to the MainView security interface, specify one of the following values in the ESM Type field:

**ACF2**
CA ACF2 is your primary ESM.

**RACF**
RACF is your primary ESM. It is only necessary to specify RACF if you also have CA ACF2 installed, but you want to use RACF.

**TSS**
CA Top Secret is your primary ESM.

**SAF**
A generic SAF interface is in use, such as one that was developed in-house.

The default value of AUTO tells MainView to determine automatically which ESM is installed and active.

6 If you use the RACF GROUP feature and you do not want it to be inherited on a connected system, specify **IGNORE** in the GROUP Inherit field.

The GROUP IDENT of a user ID is *not* inherited by a target system.

---

**NOTE**
United States Department of Defense B1 security guidelines require the GROUP Inherit value to be **ALLOW** or **UTKNONLY**.
7 Modify other default parameter values as necessary.

8 When your changes are complete, press the END key.

   The SEPDEF view is redisplayed.

9 On the COMMAND line, type SAVE and press Enter to save your parameter changes.

   The Save a Security Parameter Definition dialog is displayed.

---

**NOTE**

At any time before you enter the SAVE command, you can cancel your changes by entering CANcel on the COMMAND line. The default security parameters are reinstated.

---

10 *(optional)* In the Description field, update the existing description or specify a new description of up to 30 characters.

11 Press the END key to save the updated parameter definition member in the BBSECURE parameter library.

**To modify the BBMTSS00 parameter definition member**

1 Copy member BBMTSS from the BBACTDEF library to the BBSECURE parameter library.

2 Rename the member in BBSECURE to BBMTSS00.

   The default BBMTSS member that is distributed with MainView products contains the following statements:

```
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) */
PGRMNAME(ALLOW) /* USER CAN SPECIFY PROGRAMMER NAME */
ESMGRINH(ALLOW) /* ALWAYS ALLOW GROUP IDENT INHERITANCE */
ACCTINFO(ALLOW) /* USER CAN SPECIFY ACCOUNTING INFO. */
```
For a complete description of BBMTSS and its parameters, see the appendix of default parameter and class definitions in the *MainView Security Reference Manual*.

3 To identify a specific ESM to the MainView security interface, specify one of the following values on the **ESMTYPE** statement:

**ACF2** CA ACF2 is your primary ESM.
**RACF** RACF is your primary ESM. It is only necessary to specify RACF if you also have CA ACF2 installed, but you want to use RACF.
**TSS** CA Top Secret is your primary ESM.
**SAF** A generic SAF interface is in use, such as one that was developed in house.

The default statement, **ESMTYPE(AUTO)**, tells MainView to determine automatically which ESM is installed and active.

4 If you use the RACF GROUP feature and you do not want it to be inherited on a connected system, specify **ESMGRINH(IGNORE)**.

The GROUP IDENT of a user ID is **not** inherited by a target system.

**NOTE**

United States Department of Defense B1 security guidelines require
**ESMGRINH(ALLOW)** or **ESMGRINH(UTKNONLY)** to be specified.

5 Modify other default parameter values as necessary.

6 Save the updated BBMTSS00 member in BBSECURE.

7 Reinitialize the CAS.

Reinitializing the CAS disrupts any connected PASs and cross-system communication sessions on the local system (the CAS and all associated PASs).
For full-screen mode

The security parameters for products that run in full-screen mode are specified as control statements in a member called BBSEC. To activate security, BBSEC must reside in SYS1.PARMLIB, the logical PARMLIB concatenation, or the BBIPARM concatenation.

**TIP**
- If BBSEC is in SYS1.PARMLIB or the logical PARMLIB concatenation, all BBI-SS PASs can share the same security parameters.
- If BBSEC is in the BBIPARM concatenation (including BBPARM, UBBPARM, or TOMPARM) for one or more BBI-SS PASs, the security parameters are specific to those PASs.
- If you are running MainView SYSPROG Services outside of MainView (as a batch job or directly under TSO), the BBSEC member that contains TYPE=SYSPROG must reside in SYS1.PARMLIB or the logical PARMLIB concatenation.

To create a BBSEC member

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

**NOTE**
*Do not* add BBSEC to SYS1.PARMLIB, the logical PARMLIB concatenation, or the BBIPARM concatenation until you are ready to activate security.

2. To identify the products that you want to secure, add a TYPE statement to BBSEC for each product.

**NOTE**
This section presents the basic format of the TYPE statement with common parameters that are used by a majority of full-screen products. For a complete description of BBSEC, the TYPE statement, and all of its parameters (including additional, product-specific parameters), see the MainView Security Reference Manual.

The basic format of the TYPE statement is as follows:

```plaintext
TYPE=product, SS=ssid[.PREFIX=prefix][.CLASS=name][.FEATURE=(feature,...)]
```

where
**TYPE=product** activates security for the specified product or group of products

Specify one of the following products on each TYPE statement. You can specify as many TYPE statements as needed in a BBSEC member.

**BBI** activates security for resources that are common to MainView AutoOPERATOR, MainView FOCAL POINT, MainView for CICS, MainView for DB2, MainView for DBCTL, MainView for IMS Online, MainView for WebSphere MQ

A TYPE=BBI statement is required for these products.

**AAO** activates additional security for MainView AutoOPERATOR commands, applications, EXECs, ALERTs, and parameter data. TYPE=BBI is also required in the same BBSEC member.

**IBM CICS** activates additional security for MainView for CICS and MainView AutoOPERATOR for CICS resources. TYPE=BBI is also required in the same BBSEC member.

**IBM DB2** activates additional security for MainView for DB2 resources. TYPE=BBI is also required in the same BBSEC member.

**SYSPROG** activates security for resources that are common to MainView SYSPROG Services, MainView AutoOPERATOR, MainView for z/OS

**TOM** activates security for MainView Total Object Manager (TOM) resources.

**SS=ssid**
**SSID=ssid**

the one- to four-character subsystem ID of the BBI-SS PAS where the specified resources are to be protected

The SSID is part of the resource name that defines resources to your ESM. Each SSID that is used in a resource name must be specified on a separate TYPE statement in BBSEC.

**Notes:**
- TYPE=SYSPROG statements do not use SS=ssid.
- TYPE=TOM statements use TOMID=tom_id instead of SS=ssid.

**PREFIX=prefix** (optional, TYPE=BBI only) the one- to eight-character prefix for all MainView product resource names. The default is BBM.
CLASS=\textit{name} \hspace{1cm} \textit{(optional, TYPE=BBI only)} the one- to eight-character security class name that is used to identify MainView product resources. The default is $BOOLE$.

\textbf{FEATURE=$\left\{\text{feature},\ldots\right\}$} For MainView for DB2 (TYPE=DB2), specify

- **CMD** for DB2 command-level security

For MainView AutoOPERATOR (TYPE=AAO), specify one or more of the following values:

- **CMD** for command and transaction security
- **APPL** for application security
- **EXEC** for EXEC security
- **ALRT** for ALERTs security
- **PARM** for parameter member security
- **ALRTEXEC** for Alert Follow-up EXECs
- **IMSGEN** for IMS generic commands security (requires CMD)

The FEATURE parameter and its keywords must be specified on a single line in BBSEC. Separate multiple keywords by a comma and enclose all keywords in parentheses.

Observe the following syntax rules when creating or updating BBSEC:

- Each TYPE statement and its parameters can be specified in positions 1–72 on one or more lines.

- 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=$\left\{\text{CMD,APPL,EXEC}\right\}$ must appear on a single line.

- Specify comments on separate lines with an asterisk (*) in column 1. Comments are not supported on the same line as a TYPE statement.

3 Save the updated BBSEC member.

4 To test your security parameters

A Copy BBSEC into the BBPARM data set for a BBI-SS PAS.

B Warm start the BBI-SS PAS to read the new BBSEC member.

C Test product access at the BBI-SS PAS level to make sure that it provides the security that you want.
When you are satisfied with the way that security is working at the BBI-SS PAS level, copy (or move) BBSEC to SYS1.PARMLIB, the logical PARMLIB concatenation, or the BBIPARM concatenation for other PASs.

**NOTE**
For information about protecting the BBSEC member from unauthorized modification, see “Controlling access to security resources” on page 78.

**Sample BBSEC member**

A sample BBSEC member is shown in Figure 7.

**Figure 7  Sample BBSEC member**

```plaintext
* Activates security for common resources:
* TYPE=BBI,SS=SYSB,PREFIX=BB1,CLASS=$MAINVIEW
* Activates security for MAINVIEW for DB2 and
* DB2 command-level security:
* TYPE=DB2,SS=SYSB,FEATURE=(CMD)
```
Identifying the security class

Use the procedures in this section to identify the security class for MainView product resources to your ESM.

For windows mode

NOTE

The default security class for resources in windows mode is $BBM. By default, $BBM is transformed (by use of a NEXT statement) to external resource class FACILITY, which is a predefined class for CA ACF2, CA Top Secret, and RACF.

If you can use FACILITY as your security class, you do not need to modify the security class for windows-mode products.

If you need to use a security class other than FACILITY for products that run in windows mode, you can either

- use the SECDEF views
- modify member BBMTSP00 directly (as described on page 48)

To use the SECDEF views

1. From within Plex Manager, perform one of the following actions:

   - Use the EZSEC menu:
     1. On the COMMAND line, type EZSEC and press Enter.
     2. On the EZSEC menu, position your cursor on Review Class Definitions and press Enter.

   - On the COMMAND line, type SECDEFL and press Enter.

The SECDEFL view is displayed, as shown in Figure 8 on page 46.
Figure 8  SECDEFL view

SECDEFL is a list of security class definition members. The default member is BBMTSP00 and it appears on SECDEFL with a member suffix of 00.

2  In the CMD line command field, type S next to member suffix 00 and press Enter.

The SECDEF view is displayed, as shown in Figure 9.

Figure 9  SECDEF view

SECDEF is a list of the default security classes that are defined in member BBMTSP00. BBMTSP00 contains all known security classes for RACF, CA Top Secret, and CA ACF2.
NOTE

The first time the SECDEFL view is displayed, the Description field contains the following message:

Empty member—Select to create

When you select an empty member, the following message appears in the SECDEF view:

BBMYA923E The parameter member BBMTSP00 is missing

Disregard the message and press Enter to display the default security classes.

3 On the COMMAND line, type EDIT and press Enter to request an edit session.

4 In the CMD line command field, type C next to security class $BBM and press Enter.

The Change Security Class Definition dialog is displayed, as shown in Figure 10.

Figure 10 Change Security Class Definition dialog

For information about the fields on this dialog, press the Help key.
5 In the **Next Class** field, specify the name of the security class that you want $BBM to use instead of FACILITY.

**NOTE**

- The **Next Class** value must be different than the internal security class that is named in the **Class Name** field.

- If you want to use a security class that is not included in member BBMTSP00 (as shown in the SECDEF view), you must first define the new class and add it to a security class definition member. For information about adding a new security class, see the *MainView Security Reference Manual*.

6 When your changes are complete, press the **END** key.

The SECDEF view is redisplayed.

7 On the **COMMAND** line, type **SAVE** and press **Enter** to save your security class changes.

The Save a Security Class Definition dialog is displayed.

**NOTE**

At any time before you enter the **SAVE** command, you can cancel your changes by entering **CANCEL** on the **COMMAND** line. The default security classes are reinstated.

8 *(optional)* In the **Description** field, update the existing description or specify a new description of up to 30 characters.

9 Press the **END** key to save this security class definition member in the BBSECURE parameter library.

**To modify the BBMTSP00 class definition member**

1 Copy member BBMTSP from the BBACTDEF library to the BBSECURE parameter library.

2 Rename the member in BBSECURE to BBMTSP00.

3 Edit member BBMTSP00, as required for your ESM.

The default BBMTSP member that is distributed with MainView products contains definitions for all security classes that are known to RACF, CA Top Secret, and CA ACF2. A partial list of those definitions follows:
For a complete description of BBMTSP and all of its parameters (including ESM-specific parameters), see the appendix of default class definitions in the *MainView Security Reference Manual*. 

For full-screen mode

By default, the security class for products that run in full-screen mode is called $BOOLE. You need to define security class $BOOLE to your ESM.

To define security class $BOOLE

1 In your RACF Router Table, specify the following TSO command:

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

where $BOOLE is the default security class name.
In your RACF Resource Class Descriptor Table, specify

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

To activate the $BOOLE security class, enter the following RACF command:

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

To allow $BOOLE to use generic profiles, enter the following RACF command:

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

**Additional examples**

The examples in this section show how to define security class $BOOLE to CA ACF2 and CA Top Secret.

- For CA ACF2, use the following TSO commands to update the CLASMAP records with security class $BOOLE:

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

where `type` is a CA ACF2 resource type code.

- For CA Top Secret, use the following TSS ADDTO command to update the resource definition table (RDT) with security class $BOOLE:

```
TSS ADDTO(RDT) RESCLASS($BOOLE)+
    RESCODE(xx) ATTR(PRIVPGM,LONG,GENERIC)+
    ACLST(NONE,READ,UPDATE,ALL)+
    DEFACC(NONE)
```

where `xx` is a two-digit hexadecimal resource code. The access level information (ACLST and DEFACC) that is shown is only an example. You can choose your own access level names and default access level.
Identifying the resources to be secured

This section describes how MainView resources are named and introduces tools that you can use to identify resources to your ESM.

For windows mode

This section describes how resources are named in windows mode and how to use the SERDEF views to identify resources.

How resources are named

All product resources in windows mode (such as view data and actions) have a defined resource name. Resources that have a unique function have their own distinct resource entity name. Most resources, however, have similar functions (such as all view actions) and they share a default resource entity name that can be used for high-level control. You can enable or disable security for the default resource, and that enables or disables security for all the resources that reference the default. You can also selectively enable or disable security for individual resources, if necessary.

MainView resource entity names consist of multiple qualifiers separated by periods, similar to data set names. The format of a resource entity name is

\[ \text{BBM}.\text{product}.\text{context}.\text{internalID}.\text{suffix} \]

where

- **BBM** is the prefix for all MainView resources
- **product** is the ID of the product or service point that is in control of the window where the resource is being accessed
- **context** is the context that is set in the window where the resource is being accessed
- **internalID** is the internal ID of the data table or action that is being accessed
- **suffix** indicates the type of resource that is being accessed

See Table 2 on page 52 for a list of product IDs.

To determine the internal ID for a particular product resource, refer to the MainView Security Reference Manual. As an alternative, you can use the SERDEF views to manage MainView product resources, as described in “Using SERDEF views to identify resources” on page 54.

See Table 3 on page 53 for a list of resource entity name suffixes.
Table 2 lists the MainView product IDs that can be part of a resource entity name.

<table>
<thead>
<tr>
<th>Product ID</th>
<th>Product or service point</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMON</td>
<td>common MainView resources</td>
</tr>
<tr>
<td>PLEXMGR</td>
<td>Plex Manager</td>
</tr>
<tr>
<td>CMF</td>
<td>CMF MONITOR</td>
</tr>
<tr>
<td>MVALARM</td>
<td>MainView Alarm Manager - Alarm Administration</td>
</tr>
<tr>
<td>MVALERT</td>
<td>MainView Alarm Manager - Alert Management</td>
</tr>
<tr>
<td>MVAO</td>
<td>MainView AutoOPERATOR</td>
</tr>
<tr>
<td>TOM</td>
<td>MainView Total Object Manager</td>
</tr>
<tr>
<td>MVCICS</td>
<td>MainView for CICS</td>
</tr>
<tr>
<td>MVCSMON</td>
<td>COMMON STORAGE MONITOR</td>
</tr>
<tr>
<td>MVDAC</td>
<td>MainView for DATA ACCELERATOR Compression</td>
</tr>
<tr>
<td>MVDB2</td>
<td>MainView for DB2</td>
</tr>
<tr>
<td>MVIMS</td>
<td>MainView for IMS Online and MainView for DBCTL</td>
</tr>
<tr>
<td>MVIP</td>
<td>MainView for IP</td>
</tr>
<tr>
<td>MVMQS</td>
<td>MainView for WebSphere MQ</td>
</tr>
<tr>
<td>MVMVS</td>
<td>MainView for z/OS</td>
</tr>
<tr>
<td>MVSPS</td>
<td>MainView SYSPROG Services</td>
</tr>
<tr>
<td>MVSRM</td>
<td>MainView Storage Resource Manager (SRM)</td>
</tr>
<tr>
<td>MVSRMHSM</td>
<td>MainView SRM Reporting</td>
</tr>
<tr>
<td>MVSRMSGC</td>
<td>MainView SRM Reporting</td>
</tr>
<tr>
<td>MVSRMSGD</td>
<td>MainView SRM Reporting</td>
</tr>
<tr>
<td>MVSRMSGP</td>
<td>MainView SRM Reporting</td>
</tr>
<tr>
<td>MVUSS</td>
<td>MainView for UNIX System Services</td>
</tr>
<tr>
<td>MVP</td>
<td>MainView VistaPoint</td>
</tr>
<tr>
<td>MVVTAM</td>
<td>MainView for VTAM</td>
</tr>
<tr>
<td>MVWEB</td>
<td>MainView for WebSphere Application Server</td>
</tr>
</tbody>
</table>
Table 3 lists the resource suffixes that can be part of a resource entity name.

**Table 3  Suffixes for resource entity names in windows mode**

<table>
<thead>
<tr>
<th>Suffix</th>
<th>Resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>any action for a given product</td>
</tr>
<tr>
<td>AO</td>
<td>any action on the current table of data</td>
</tr>
<tr>
<td>CN</td>
<td>connection to a CAS, which provides access to the MAINVEW environment</td>
</tr>
<tr>
<td>OA</td>
<td>any action on an object in a table, such as a row of data</td>
</tr>
<tr>
<td>OD</td>
<td>table data and the views that display the data</td>
</tr>
<tr>
<td>PA</td>
<td>any product-level (or primary) action</td>
</tr>
<tr>
<td>PF</td>
<td>a product-level function</td>
</tr>
<tr>
<td>PS</td>
<td>a product-level service or agent activity</td>
</tr>
<tr>
<td>TA</td>
<td>access to a target context, which controls access to a product from the MainView Selection Menu</td>
</tr>
<tr>
<td>TC</td>
<td>creation of a target context, which allows an address space to define itself as a product</td>
</tr>
<tr>
<td>TH</td>
<td>setting of global thresholds</td>
</tr>
<tr>
<td>TS</td>
<td>granting of trusted status to a PAS for inheriting a security environment</td>
</tr>
</tbody>
</table>

Products that run in windows mode generally have from one to five default resource entity definitions. All other resource entity definitions inherit their characteristics from these defaults. This structure makes it easy to manage a large number of resource entities without having to modify each definition individually.

The default resource entity definitions are shown in **Table 4**.

**Table 4  Default resource entity definitions for products in windows mode**

<table>
<thead>
<tr>
<th>Resource name</th>
<th>Resource entity definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default - Table Data</td>
<td>BBM.product.targetid.tableid.OD</td>
</tr>
<tr>
<td>Default - Any Table Actions</td>
<td>BBM.product.targetid.tableid.AO</td>
</tr>
<tr>
<td>Default - Primary Actions (All Views)</td>
<td>BBM.product.targetid.actionid.PA</td>
</tr>
<tr>
<td>Default - Specific Table Actions</td>
<td>BBM.product.targetid.tableid.actionid.OA</td>
</tr>
<tr>
<td>Any Action (Product Views)</td>
<td>BBM.product.targetid.AA</td>
</tr>
<tr>
<td>Default - Alter Data Set</td>
<td>dsname</td>
</tr>
</tbody>
</table>
For windows mode

Using SERDEF views to identify resources

Each MainView product that runs in windows mode has SERDEF administrative views for its resource definitions. The SERDEF views can be used to review and change the distributed resource definitions.

1. On the COMMAND line of any MainView product that runs in windows mode, type SERDEFL and press Enter.

The SERDEFL view is displayed, as shown in Figure 11.

**Figure 11  SERDEFL view**

```
<table>
<thead>
<tr>
<th>ddmmmyyy hh:mm:ss</th>
<th>MAINVIEW WINDOW INTERFACE (Vv.r.mm)</th>
<th>SCROLL ===</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAND ===</td>
<td>ALT WIN ===&gt;</td>
<td>W1 =SERDEFL=</td>
<td>SYSC=</td>
</tr>
<tr>
<td>CURR WIN ===&gt; 1</td>
<td>CMD Member Product</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--- Suffix -------- ------------</td>
<td>COMMON MAINVIEW Common Resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 PLEXMGR Plex Manager Resources</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

SERDEFL displays a list of resource definition members for the current product. When the product is Plex Manager, the resource definition members for Plex Manager and common MainView resources are both displayed.

**NOTE**

From the EZSEC menu, you can hyperlink on the following fields:

- **Common Resources** to display the SERDEFL view with only the COMMON resource definition member
- **Product Resources** to display the EZSECRES menu, which enables you to select another context or product and display those resource definitions

2. To review the common resource definitions, in the CMD line command field next to COMMON type S and press Enter.

The SERDEFOV view is displayed, as shown in Figure 12 on page 55.
SERDEFOV lists each resource definition for the current context and product, and indicates whether the resource definition is enabled. Three plus signs (+++) in the Exp field indicate a default resource definition, which controls multiple individual resource definitions. From SERDEFOV, you can

- enable, disable, or change a default resource definition to affect all the individual definitions that reference the default

- manage individual resource definitions that reference a default by placing the cursor on the +++ in the Exp field and pressing Enter to display the SERDEFEX view

**NOTE**

The first time the SERDEFL view is displayed, the Description field contains the following message:

Empty member--Select to create

When you select an empty member, the following message appears in the SERDEFOV view:

BBMYA216W Parameter member xxxxRN00 is missing

where xxxx is a product-specific identifier (such as BBMZRN00 for the common resources).

Disregard the message and press Enter to display the default resource definitions.

3 On the COMMAND line, type EDIT and press Enter to request an edit session.
4 (optional) To enable or disable a resource definition, in the CMD line command field next to the definition, type one of the following commands and press Enter:

**ENA** to enable a resource definition that is currently disabled

When a resource definition is enabled, security calls can be made to your ESM for that resource.

**DIS** to disable a resource definition that is currently enabled

When a resource definition is disabled, no security calls can be made to your ESM for that resource.

5 (optional) To change the security class, resource entity name, access intent, or log options of a resource definition, in the CMD line command field next to the definition type Cha and press Enter.

The Change Security Resource Definition dialog is displayed, as shown in Figure 13.

**Figure 13** Change Security Resource Definition dialog

For information about the fields on this dialog, press the HELP key.

6 When your changes are complete, press the END key.

The SERDEFOV view is redisplayed.
7 On the **COMMAND** line of the SERDEFOV view, type **SAVE** and press **Enter** to save your resource definition changes.

The Save Security Resource Definitions dialog is displayed.

---

**NOTE**
At any time before you enter the SAVE command, you can cancel your changes by entering **CANCEL** on the **COMMAND** line. The previous resource definitions are reinstated.

---

8 *(optional)* In the **Description** field, update the existing description or specify a new description of up to 30 characters.

9 Press the **END** key to save this resource definition member in the BBSECURE parameter library.

10 *(optional)* Repeat this task of enabling, disabling, or changing resource definitions for Plex Manager and each MainView product that runs in windows mode at your site.

---

**NOTE**
The SERDEF resource definition views (SERDEFL, SERDEFOV, SERDEFEX and others) can be issued from any MainView product in windows mode. The resource definitions (or the member) for the current product are displayed.

---

**For full-screen mode**

This section describes how resources are named in full-screen mode and how to use distributed CLISTs to identify resources.

**How resources are named**

Security for full-screen products involves securing resources on a PAS-by-PAS basis. The BBI-SS PAS subsystem name and target system are part of the resource name; they determine the PAS and target system for which the particular resource is secured.

The resource naming convention for most full-screen products is

```
prefix.ssid.product.target.suffix
```

where
For full-screen mode

prefix is the one- to eight-character prefix that is used for product resource names in full-screen mode

If you do not specify a prefix, the default prefix of BBM is added to all resource names automatically.

ssid is the one- to four-character subsystem ID of the BBI-SS PAS that is being secured

Subsystem IDs for BBI-SS PASs are specified in BBPARM member BBJNT00.

product is one of the following product abbreviations:

- BBI for common resources
- AAO for MainView AutoOPERATOR resources
- CICS for MainView for CICS resources
- DMR for MainView for DB2 resources

target is the one- to eight-character name of the target system that is being secured

Target system names are specified in BBPARM member BBJNT00.

suffix is a predefined suffix that represents a specific resource

NOTE
MainView Total Object Manager (TOM), MainView SYSPROG Services, and COMMON STORAGE MONITOR (CSM) use slightly different resource naming conventions. For information about resource names for those products, refer to the MainView Security Reference Manual.

When you create rules, profiles, or permits to control access to resources, you can specify an explicit or generic value for any qualifier in the resource name except the prefix. For example, an explicit resource name might look like

BBM.SS01.AAO.SS01.RULEREAD

To use generic values, first make sure that your ESM and the security class that you defined to it support the use of generics. The * represents a string of characters.

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

BBM.SS01.CICS.CICS*.FILE.*

controls access to all CICS display file services on target systems whose names begin with CICS.
Using CLISTs to identify resources

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

Creating resource names for MainView products

To define common, full-screen product resources to RACF, use the RACFDEF CLIST. The RACFDEF CLIST prompts you to enter the following information:

- prefix to use as the high-level qualifier for each resource name (BBM is the default)
- security class to use ($BOOLE is the default)
- subsystem ID of the BBI-SS PAS that you are securing
- default access rights for all the resources (READ or NONE)
- target that you are securing (as defined in BBPARM member BBIJNT00)

You should run the RACFDEF CLIST once for every BBI-SS PAS and for every target that you are securing.

Migrating existing resource names

If you want to migrate resource names that were previously defined with BMC Software proprietary security, use the MIGUSER CLIST.

**NOTE**

If you are still using BMC Software proprietary security, refer to the *MainView Security Reference Manual*.

The MIGUSER CLIST prompts you to enter the following information:

- subsystem ID of the BBI-SS PAS that you are securing
- prefix to use as the high-level qualifier for each resource name (BBM is the default)
- security class to use ($BOOLE is the default)
- user ID to migrate
- BBPARM data set where the $USERID member that you are converting resides

The definitions in member $USERID must be syntactically correct for the MIGUSER CLIST to run successfully. The $USERID member should not include any generic AUTHJOB definitions unless the specified security class was implemented as a generic class. The value specified in the AUTHJOB keyword is equivalent to the target node of the resource name.
Disabling security

Additional CLISTs for identifying resources

To identify additional, product-specific resources to your ESM, use the following CLISTs:

<table>
<thead>
<tr>
<th>Product</th>
<th>CLIST name</th>
<th>Resources for</th>
</tr>
</thead>
<tbody>
<tr>
<td>MainView AutoOPERATOR</td>
<td>AOANYDF, AOANYPE</td>
<td>AOAAnywhere facility</td>
</tr>
<tr>
<td></td>
<td>AOCMDDF, AOCMDPE</td>
<td>CMD feature</td>
</tr>
<tr>
<td></td>
<td>AOAPPLDF, AOAAPLPE</td>
<td>APPL feature</td>
</tr>
<tr>
<td></td>
<td>AOALRTDF, AOALRTPE</td>
<td>ALRT feature</td>
</tr>
<tr>
<td></td>
<td>AOEXECDF, AOEXECPE</td>
<td>EXEC feature and ALRTEXEC feature</td>
</tr>
<tr>
<td></td>
<td>AOPARMDF, AOPARMPE</td>
<td>PARM feature</td>
</tr>
<tr>
<td>MainView for CICS</td>
<td>CICSRACF</td>
<td>CICS functions</td>
</tr>
<tr>
<td>MainView for DB2</td>
<td>DB2CMDDF, DB2CMDPE</td>
<td>CMD feature</td>
</tr>
</tbody>
</table>

Disabling security

You can disable security completely if you decide that you do not need to restrict access to MainView product resources at your site. Use the procedures in this section to disable security.

For windows mode

If you decide to disable security for products that run in windows mode, you can either

- use the SEPDEF views
- modify member BBMTSS00 directly (as described on page 61)

**NOTE**

If you disable security in windows mode by specifying an ESM type of NONE, MainView bypasses security for the entire subsystem (the CAS and all associated PAs).
To use the SEPDEF views

1. From within Plex Manager, type SEPDEFL on the COMMAND line and press Enter.

2. In the CMD line command field of the SEPDEFL view, type S next to the parameter definition member that you want to disable and press Enter.

   The SEPDEF view is displayed.

3. On the COMMAND line, type EDIT and press Enter to request an edit session.

4. On the COMMAND line, type CHAnge and press Enter.

   The Change Global Security Parameters dialog is displayed.

5. In the ESM Type field, type NONE and press the END key.

6. On the COMMAND line of the SEPDEF view, type SAVE and press Enter to save your change.

7. Exit your MainView session and reinitialize the CAS.

   Reinitializing the CAS disrupts any connected PASs and cross-system communication sessions on the local system (the CAS and all associated PASs).

To modify the BBMTSS00 parameter definition member

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

   If a BBMTSS00 member contains security parameters that you want to keep, rename the member to something else.

2. Create a new member called BBMTSS00 in the BBSECURE parameter library.

3. Add the following statement to the new BBMTSS00 member:

   ESM ESMTYPE(NONE);

4. Save the new BBMTSS00 member.

5. Reinitialize the CAS.

   Reinitializing the CAS disrupts any connected PASs and cross-system communication sessions on the local system (the CAS and all associated PASs).
Disabling security for products that run in full-screen mode involves modifying the BBSEC member.

**To disable security for one or more specific products**

1. In the BBSEC member in both the logical PARMLIB concatenation and the BBIPARM concatenation, change the TYPE statements for the appropriate products to comments by typing an asterisk (*) in column one.

2. Warm start each affected BBI-SS PAS.

**To disable security for all products**

1. Perform one of the following tasks:
   - Remove the BBSEC member from both the logical PARMLIB concatenation and the BBIPARM concatenation.
   - Rename all BBSEC members to a different name.

2. Warm start each affected BBI-SS PAS.
How to control access to resources

You can control access to a wide range of MainView resources, from the CAS, PAS or target system as a whole, to specific types of data or specific actions within a product. In addition, it is important that you restrict access to the resources that control MainView security.

This chapter presents procedures for completing the following tasks:

Controlling access to the CAS ................................................................. 64
  Globally securing all CASs ............................................................... 65
  Securing individual CASs ............................................................... 65
Controlling access to PASs and target systems ....................................... 66
Controlling access to product data ....................................................... 67
  In windows mode ........................................................................... 68
  In full-screen mode ....................................................................... 70
Controlling access to product actions .................................................... 71
  In windows mode ........................................................................... 72
  In full-screen mode ....................................................................... 73
Controlling MainView Alternate Access ................................................... 75
Controlling access to security resources ............................................... 78
  For windows mode ........................................................................ 78
  For full-screen mode ..................................................................... 79
Controlling access to the CAS

**NOTE**

This section applies to products that run (either in whole or in part) in windows mode.

Products that run in windows mode rely on the CAS for communication among address spaces and terminal session users. When you control access to the CAS, you are controlling access to all MainView products that run in windows mode.

Depending on the level of security that you want at your site, you can define

- a single rule, profile, or permit for access to all CASs
- individual rules, profiles, or permits for each CAS subsystem ID

Access to one or more CASs is controlled by the following resource:

**BBM.ssid.CN**

where *ssid* is a specific or generic CAS subsystem ID.

**NOTE**

In the SERDEF view for Common MainView resources, the CAS access resource is called **Global - Connect to CAS**.
Globally securing all CASs

Defining a single rule, profile, or permit to secure the Global - Connect to CAS resource works best for sites that are basically open, where

- in general, everybody is granted access to everything
- only outsiders are denied access

Examples

<table>
<thead>
<tr>
<th>For this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF</td>
<td>FACILITY BBM.*.CN</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) TYPE(FAC) *-.CN</td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.*.CN)</td>
</tr>
</tbody>
</table>

Securing individual CASs

If your site is basically closed and you want to control access to specific CASs (such as a production CAS or a test CAS), you can define individual rules, profiles, and permits for each CAS subsystem ID.

Examples

<table>
<thead>
<tr>
<th>For this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF</td>
<td>FACILITY BBM.C002.CN</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) TYPE(FAC) C002.CN</td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.C002.CN)</td>
</tr>
</tbody>
</table>
Controlling access to PASs and target systems

**NOTE**
This section applies to the following products, which run (either in whole or in part) in full-screen mode:

- MainView AutoOPERATOR
- MainView FOCAL POINT
- MainView for CICS
- MainView for DB2
- MainView for DBCTL
- MainView for IMS Online
- MainView for WebSphere MQ

Products that run in full-screen mode rely on PASs for various services such as data collection. When you control access to a BBI-SS PAS, you are controlling access to the specific MainView products that the PAS supports. You can also control access to one or more target systems where those products run.

Access to BBI-SS PASs, target systems, or both is controlled by the following resource:

```
prefix.ssid.BBI.target.ACCESS
```

where

- **prefix** is the one- to eight-character prefix that is used for product resource names in full-screen mode
- **ssid** is the one- to four-character subsystem ID of the BBI-SS PAS that is being secured
- **target** is the one- to eight-character name of the target system that is being secured

**NOTE**
Securing the ACCESS resource is a prerequisite to implementing security for any other full-screen product resource. Access to the BBI-SS PAS or target system is always checked before access to a specific product resource is checked.

To control access to all full-screen products (or parts of products) on all target systems, specify the ACCESS resource as follows:

```
BBM.*.BBL.*.ACCESS
```

The asterisks in the **ssid** and **target** positions of this resource name represent all BBI-SS PASs and all target systems.
To control access to the products that are running on a specific PAS, specify the following resource:

**BBM.SS01.BBI.*.ACCESS**

This resource name represents the BBI-SS PAS called SS01 and all target systems that are connected to that PAS.

### Examples

<table>
<thead>
<tr>
<th>For this ESM</th>
<th>Specify resource names such as these</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF</td>
<td>FACILITY BBM.%<em>.BBI.%</em>.ACCESS</td>
</tr>
<tr>
<td></td>
<td>FACILITY BBM.BB%%.BBI.SS*.ACCESS</td>
</tr>
<tr>
<td></td>
<td>FACILITY BBM.BBCS.BBI.SS01.ACCESS</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) TYPE(FAC)</td>
</tr>
<tr>
<td></td>
<td><em>-.BBI.</em>-.ACCESS</td>
</tr>
<tr>
<td></td>
<td>$KEY(BBM) TYPE(FAC)</td>
</tr>
<tr>
<td></td>
<td>BB**.BBI.SS**.ACCESS</td>
</tr>
<tr>
<td></td>
<td>$KEY(BBM) TYPE(FAC)</td>
</tr>
<tr>
<td></td>
<td>BBCS.BBI.SS01.ACCESS</td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.BBI.</em>.ACCESS)</td>
</tr>
<tr>
<td></td>
<td>IBMFAC(BBM.BB++.BBI.SS++.ACCESS)</td>
</tr>
<tr>
<td></td>
<td>IBMFAC(BBM.BBCS.BBI.SS01.ACCESS)</td>
</tr>
</tbody>
</table>

### Controlling access to product data

The data that is provided by MainView products can be useful to a variety of people, from end users and help desk personnel to operators and system programmers. You can decide what type of data each user is allowed to display.

---

**TIP**

- If you want to allow most users to see MainView data, start with Universal Access READ and then selectively protect views of data within a product.

- If you want to prevent most users from seeing MainView data, start with Universal Access NONE and then grant selected users access to the data.

This section describes how to control what data users can see when they use MainView products.
In windows mode

Products that run in windows mode collect tables of data and present views of that data in one or more windows.

Access to the data that is displayed in product views is controlled by the following resource:

\[ \text{BBM.product.context.tableID.OD} \]

where

- **product** is the ID of the product or service point that is in control of the window
- **context** is the context that is set in the window
- **tableID** is the internal ID of the data table

To determine the internal ID for a particular product data table, refer to the *MainView Security Reference Manual*. As an alternative, you can use the SERDEF views to manage MainView product resources, as described in “Using SERDEF views to identify resources” on page 54.

**OD** represents table data and the views that display the data

To control access to all product data and the views in which the data is displayed, specify the following resource:

\[ \text{BBM.*.*.*.OD (or BBM.*.*.OD)} \]

The asterisks in the **product**, **context**, and **tableID** positions of this resource name represent all data tables for all windows-mode products running in any context.

To control access to the data and views of a specific product, specify the product in the resource name as follows:

\[ \text{BBM.MVMVS.*.*.OD} \]

This resource name represents all MainView for z/OS data tables and views.

To protect a specific data table and its associated views, specifying a resource name such as

\[ \text{BBM.*.*.MYA40.OD} \]

This resource name represents the diagnostic message facility and the DIAGMSG view, which are available to all MainView products. MYA40 is the internal ID of the DIAGMSG data table.
In windows mode

**NOTE**
For a complete list of the resources that can be secured for windows-mode products, either
- use the SERDEF views, as described in “Using SERDEF views to identify resources” on page 54
- refer to the MainView Security Reference Manual (includes the internal IDs)

## Examples

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>All MainView product data tables and views</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.</em>.*.OD</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) TYPE(FAC) <em>-</em>-<em>-</em>-.OD</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.</em>.*.OD)</td>
</tr>
<tr>
<td>All data tables and views for a specific MainView product</td>
<td>RACF</td>
<td>FACILITY BBM.MVIMS.<em>.</em>.OD</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) TYPE(FAC) MVIMS.<em>-</em>-.OD</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.MVIMS.<em>.</em>.OD)</td>
</tr>
<tr>
<td>Specific data table for all products in any context (such as historical data sets and the DLIST view, which has an internal ID of MYAG0)</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.</em>.MYAG0.OD</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) TYPE(FAC) <em>-</em>-*MYAG0.OD</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.</em>.MYAG0.OD)</td>
</tr>
<tr>
<td>Specific data table and views for a specific product in any context</td>
<td>RACF</td>
<td>FACILITY BBM.MVDB2.*.SP630.OD</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) MVMS.*-.DC201.OD</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.MVSRM.*.WB100.OD)</td>
</tr>
</tbody>
</table>
In full-screen mode

For products that run in full-screen mode you can control access to resources on a given PAS or target system. You can further refine your security by controlling access to the commands and functions that are provided by a specific product.

Access to all commands and functions for a given product is controlled by the following resource:

\[ \text{BBM.*.product.*.*.*} \]

where \textit{product} can be one of the following values:

- \textbf{AAO} \hspace{1cm} \text{MainView AutoOPERATOR}
- \textbf{BBI} \hspace{1cm} \text{common resources}
- \textbf{CICS} \hspace{1cm} \text{MainView for CICS and MainView AutoOPERATOR for CICS}
- \textbf{DMR} \hspace{1cm} \text{MainView for DB2}

\textbf{NOTE}

MainView FOCAL POINT, MainView for DBCTL, MainView for IMS Online, and MainView for WebSphere MQ do not have any specific, full-screen resources to be secured. Access to the full-screen portions of these products is controlled by the BBI common resources.

To control access to all MainView for CICS and MainView AutoOPERATOR for CICS resources, specify the following resource:

\[ \text{BBM.*.CICS.*.*.*} \]

To control access to a specific product function, specify a resource name such as

\[ \text{BBM.*.AAO.*.RULEREAD} \]

This resource controls the ability to display the MainView AutoOPERATOR Rules Processor application.

\textbf{NOTE}

For a complete list of the resources that can be secured for full-screen products, refer to the \textit{MainView Security Reference Manual}. 

---

\textit{MainView Security Guide}
Examples

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>All resources for a specific MainView product</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.AAD.</em>.*</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.CICS.</em>-.*-</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.DMR.</em>.*.)</td>
</tr>
<tr>
<td>BBI-SS PAS journal for any PAS and any target system</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.BBI.</em>.JRNLMSG</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.BBI.</em>-.JRNLMSG)</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.BBI.</em>.JRNLMSG)</td>
</tr>
<tr>
<td>Specific product resource on selected systems (such as MainView for DB2 SQL text on systems whose name begins with PR)</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.DMR.PR</em>.DB2SQLAL</td>
</tr>
<tr>
<td></td>
<td>CA ACF2</td>
<td>$KEY(BBM) *-.DMR.PR-.DB2SQLAL</td>
</tr>
<tr>
<td></td>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.DMR.PR</em>.DB2SQLAL)</td>
</tr>
</tbody>
</table>

Controlling access to product actions

Controlling what actions users can take against MainView resources is probably more important to you than controlling what data they can see. Some MainView product actions provide the ability to add, change, and delete not only MainView resources, but also system and subsystem resources.

**TIP**

If you want to prevent most users from being able to modify the system resources that MainView monitors, you should specify Universal Access NONE for all action resources.

This section describes how to control what actions users can perform when they use MainView products.
In windows mode

Products that run in windows mode offer many actions that users can perform against a whole table of data or a specific object within a table.

The ability to issue action commands against a table of data is controlled by the following resource:

\[ \text{BBM}. \text{product}. \text{context}. \text{tableID}. \text{AO} \]

where

- \textit{product} is the ID of the product or service point that is in control of the window
- \textit{context} is the context that is set in the window
- \textit{tableID} is the internal ID of the data table

To determine the internal ID for a particular product data table, refer to the \textit{MainView Security Reference Manual}. As an alternative, you can use the SERDEF views to manage MainView product resources, as described in “Using SERDEF views to identify resources” on page 54.

\textit{AO} represents any action on the specified table of data

The ability to issue a specific action command against an object in a table of data is controlled by the following resource:

\[ \text{BBM}. \text{product}. \text{context}. \text{tableID}. \text{actionID}. \text{OA} \]

where

- \textit{actionID} is the name of the action

To determine the name of a particular action, use the SERDEF views (as described in “Using SERDEF views to identify resources” on page 54) or refer to the \textit{MainView Security Reference Manual}.

\textit{OA} represents any action on an object in a table, such as a row of data

\hspace{1cm} \textit{NOTE}\hspace{1cm}

Some products also have a \textit{BBM}.\textit{product}.\textit{context}.\textit{tableID}.\textit{AA} resource, which controls access to any action command for the product, at either the data table level or the object level.
To control access to all action commands for all tables of MainView product data, specify the following resource:

**BBM.*.*.*.*.AO**

This resource name represents all actions against all data tables for windows-mode products running in any context.

To control access to the action commands for a specific product, specify the product name as follows:

**BBM.MVIMS.*.*.AO**

This resource name represents all actions against MainView for IMS Online and MainView for DBCTL data tables in any context.

To protect the actions for a specific table of product data, specify a resource name such as

**BBM.MVMVS.*.DCE15.AO**

This resource name represents all actions against MainView for z/OS MVScope data. It is also possible to prevent users from collecting or viewing MVScope I/O data in the first place by specifying the following resource:

**BBM.MVMVS.*.MVSCPDAT.PA**

For more information about controlling access to the MVScope facility, refer to the *MainView for z/OS User Guide and Reference*.

---

**In full-screen mode**

Some MainView full-screen products have actions that you might want to secure separately from other product resources. In general, full-screen resource names look like this example:

**BBM.ssid.product.target.suffix**

The *suffix* is what distinguishes display-only resources from actions.
If you previously secured all the resources for a given product (by denying access to BBM.*.product.*.*.*), the action commands for that product are secure. However, if you granted access to all or most product resources, you should further secure those resources that represent potentially harmful actions.

For example, some MainView for CICS actions enable users to modify CICS system values and purge CICS resources. To control access to these actions in both windows and full-screen mode, specify the following resource:

**BBM.*.CICS.*.ALT***

All MainView for CICS actions use ALT (as in alter) in the suffix portion of their resource name (such as, BBM.ssid.CICS.target.ALTTRAN.PURTRAN for the Purge Transaction action). By controlling access to BBM.*.CICS.ALT*, you are securing all MainView for CICS (and MainView AutoOPERATOR for CICS) actions in all PASs and target systems.

**NOTE**

Some MainView for CICS actions are common to

- MainView for CICS windows-mode views
- MainView for CICS full-screen mode displays
- MainView AutoOPERATOR for CICS IMFEXEC API and Rules Processor

You can control access to these actions from any source by securing the full-screen mode resources (BBM.*.CICS.*.ALTxxx.action). As distributed, the resource definitions for the equivalent windows-mode actions are disabled. For a complete list of the actions that are common to MainView for CICS and MainView AutoOPERATOR for CICS, refer to the MainView Security Reference Manual.
Examples

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>All MainView for CICS and MainView AutoOPERATOR for CICS actions in both windows and full-screen mode</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.CICS.</em>.ALT*.*</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.CICS.</em>-.ALT-.*-</td>
<td></td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.CICS.</em>.ALT*.*))</td>
<td></td>
</tr>
</tbody>
</table>

Issuing BBI control commands (such as .RESET, .CANCEL, or .START) for any PAS or target system

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuing BBI control commands (such as .RESET, .CANCEL, or .START) for any PAS or target system</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.BBI.</em>.BBICMD</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.BBI.</em>-.BBICMD</td>
<td></td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.BBI.</em>.BBICMD)</td>
<td></td>
</tr>
</tbody>
</table>

Issuing DB2 commands in MainView for DB2

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuing DB2 commands in MainView for DB2</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.DMR.</em>.DB2CMD</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.DMR.</em>-.DB2CMD</td>
<td></td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.DMR.</em>.DB2CMD)</td>
<td></td>
</tr>
</tbody>
</table>

Issuing IBM MVS™ commands from a MainView AutoOPERATOR terminal session

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuing IBM MVS™ commands from a MainView AutoOPERATOR terminal session</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.AAO.</em>.MVSCMD</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.AAO.</em>-.MVSCMD</td>
<td></td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.AAO.</em>.MVSCMD)</td>
<td></td>
</tr>
</tbody>
</table>

All SYSPROG action services from MainView for z/OS

<table>
<thead>
<tr>
<th>To control access to</th>
<th>With this ESM</th>
<th>Specify this resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>All SYSPROG action services from MainView for z/OS</td>
<td>RACF</td>
<td>FACILITY BBM.<em>.RESOLVE.</em>.UPDATE</td>
</tr>
<tr>
<td>CA ACF2</td>
<td>$KEY(BBM) <em>-.RESOLVE.</em>-.UPDATE</td>
<td></td>
</tr>
<tr>
<td>CA Top Secret</td>
<td>IBMFAC(BBM.<em>.RESOLVE.</em>.UPDATE)</td>
<td></td>
</tr>
</tbody>
</table>

Controlling MainView Alternate Access

Security for MainView Alternate Access is independent of other MainView product security. MainView Alternate Access

- uses the standard SAF interface to communicate with your ESM
- requires that each user ID for a session be defined to your ESM

NOTE

MainView Alternate Access supports AutoLogon sessions, which sign on a terminal directly to a product service at terminal address space (TAS) initialization without requiring the user to enter a user ID or password. Because of this AutoLogon feature, it is important to restrict access to MainView Alternate Access.
To control access to MainView Alternate Access

1 Define resource BOOLEBBV to your ESM with a Universal Access of NONE.

For example, for RACF specify the following TSO command:

`RDEFINE FACILITY (BOOLEBBV) UACC(NONE)`

**NOTE**

If resource BOOLEBBV is not defined to your ESM, the user ID and password must be manually specified in clear text in either the START command or the BBVTASxx member.

2 Permit each user ID that will use an AutoLogon session to have READ access to resource BOOLEBBV.

For RACF specify the following TSO command:

`PERMIT BOOLEBBV CLASS(FACILITY) ID(userID) ACCESS(READ)`

For more detailed information about MainView Alternate Access security, including information about defining additional security for terminals or applications, see the MainView Security Reference Manual.

Additional examples

The examples in this section show how to use CA ACF2 and CA Top Secret to protect resource BOOLEBBV.

- For CA ACF2, use the following TSO commands to define resource BOOLEBBV and allow selected user IDs to access it:

  ```
  ACF
  SET RESOURCE(FAC)
  COMPILE * LIST STORE
  $KEY(BOOLEBBV) TYPE(FAC)
      UID(UUID string) ALLOW
      UID(-) PREVENT
  END
  END
  ```

- For CA Top Secret, use the following TSS ADDTO command to add resource BOOLEBBV to class IBMFAC:

  `TSS ADDTO(owner-acid) IBMFAC(BOOLEBBV)`
Use the following TSS PERMIT command to permit selected ACIDs to have READ access to BOOLEBBV:

TSS PERMIT(\textit{acid}) IBMFAC(BOOLEBBV) ACCESS(READ)
Controlling access to security resources

To prevent unauthorized changes to your security environment, you should restrict access to the resources that control the MainView security interface. Security resources include resources that allow a user to change security parameters and definitions or turn off SAF security calls. Use the procedures in this section to control access to security resources.

For windows mode

Security for products that run in windows mode can be controlled by certain Plex Manager views and actions. You should restrict access to these Plex Manager resources.

To protect Plex Manager resources

1. Specify Universal Access NONE for the Plex Manager resources that are listed in Table 5.

<table>
<thead>
<tr>
<th>Resource name</th>
<th>Name in SERDEF view</th>
<th>What is protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBM.PLEXMGR.*.CYA90.OD</td>
<td>SecDef Security Class - Table Data</td>
<td>SECDEF views</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYA90.AO</td>
<td>SecDef Security Class - Any Action</td>
<td>SECDEF actions</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYAAO.OD</td>
<td>SecDef List - Table Data</td>
<td>SECDEFL view</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYAAO.AO</td>
<td>SecDef List - Any Action</td>
<td>SECDEFL actions</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYA80.OD</td>
<td>SecParm Definitions - Table Data</td>
<td>SEPDEF views</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYA80.AO</td>
<td>SecParm Definitions - Any Action</td>
<td>SEPDEF actions</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYAEO.OD</td>
<td>SecParm Def List - Table Data</td>
<td>SEPDEFL view</td>
</tr>
<tr>
<td>BBM.PLEXMGR.*.CYAEO.AO</td>
<td>SecParm Def List - Any Action</td>
<td>SEPDEFL actions</td>
</tr>
<tr>
<td>BBM.COMMON.*.MYA20.OD</td>
<td>Security Resources - Table Data</td>
<td>SERDEF views</td>
</tr>
<tr>
<td>BBM.COMMON.*.MYA20.AO</td>
<td>Security Resources - Any Action</td>
<td>SERDEF actions</td>
</tr>
<tr>
<td>BBM.COMMON.*.MYA30.OD</td>
<td>SecResource List - Table Data</td>
<td>SERDEFL view</td>
</tr>
<tr>
<td>BBM.COMMON.*.MYA30.AO</td>
<td>SecResource List - Any Action</td>
<td>SERDEFL actions</td>
</tr>
</tbody>
</table>

2. Grant selected users WRITE access to the resources listed in Table 5.
For full-screen mode

Security for products that run in full-screen mode is controlled by member BBSEC in your parameter library. You should restrict access to the BBSEC member.

**To protect the BBSEC member**

1. Specify Universal Access NONE for any BBSEC member that resides in
   - SYS1.PARMLIB
   - logical PARMLIB concatenation
   - BBIPARM concatenation

2. Grant selected users WRITE access to the BBSEC members.
Troubleshooting security problems

If your MainView security environment is not producing the expected results, you can use a variety of tools to diagnose the problem.

This chapter presents the following topics:

- Troubleshooting in windows mode .................................................. 82
  - Determining which security members are active .......................... 82
  - Using Plex Manager security tracing options .............................. 86
- Troubleshooting in full-screen mode .............................................. 87
  - Verifying the status of full-screen security ................................. 88
  - Checking MainView AutoOPERATOR advanced security ............... 89
  - Checking MainView for CICS security ....................................... 91
- Troubleshooting in MainView Explorer ......................................... 92
Troubleshooting in windows mode

This section describes how to

- determine which security members are being used for windows-mode security
- use Plex Manager tracing options to diagnose a security problem

Determining which security members are active

During CAS and PAS initialization, the parameter, class, and resource definition members in the BBSECURE parameter library are read to establish the MainView security environment. Multiple versions of a security member can exist, each having a unique suffix (the default is 00). This section explains how to determine which security members are active for the CAS and PAS.

To identify the CAS security members

1. On the COMMAND line from within Plex Manager, type CASDEF and press Enter.

2. In the CASDEF view, place the cursor on the name of the CAS in the CAS Name field and press Enter.

   The CASDEFD view is displayed, as shown in Figure 14 on page 83.
3 Review the following fields of the Parmlib Suffixes section:

- **SepDef Suffix**
  - two-character suffix of the security parameter definition member (BBMTSSnn)

- **SecDef Suffix**
  - two-character suffix of the security class definition member (BBMTSPnn)

- **Common SerDef**
  - two-character suffix of the security resource definition member for common resources (BBMZRNnn)

4 To display the contents of a security member, place the cursor in one of the Parmlib Suffixes fields and press Enter.

Depending on which field you select, one of the following views is displayed:

- **SEPDEF**
  - displays the current security parameter definition member for the CAS

- **SECDEF**
  - displays the current security class definition member that is used for all common, Plex Manager, and product-specific resources

- **SERDEF**
  - displays the current security resource definition member that is used for common and Plex Manager resources
To identify the PAS security members

1. On the COMMAND line from within Plex Manager, type CASDEF and press Enter.

2. In the CASDEF view, place the cursor on the name of the CAS to which the PAS connects in the CAS Name field and press Enter.

The CASDEFD view is displayed, as shown in Figure 15.

Figure 15  CASDEF view, PAS security suffix

3. Look at the TgtDef Suffix field of the Parmlib Suffixes section.

The TgtDef Suffix field shows the two-character suffix of the target definition member in the security parameter library that is defined to the CAS. A target definition member specifies

- a target for a specific product, such as Plex Manager on SYSA
- the resource definition member for that product

4. To display the contents of the target definition member, place the cursor in the TgtDef Suffix field and press Enter.

The TGTDEF view is displayed.
5 In the TGTDEF view, perform the following steps:

A  Look in the **Product** field for the product whose security definitions you want to review.

B  Place the cursor in the **Target Name** field for that product and press **Enter**.

The TGTDEFD view is displayed, as shown in **Figure 16**.

**Figure 16  TGTDEFD view, resource definition member suffix**

6 Check the suffix value in the **SerDef Suffix** field of the **Security Info** section.

The **SerDef Suffix** field shows the two-character suffix of the resource definition member that is being used for the product that is named in the **Product** field.

7 To display the contents of the resource definition member for that product, perform the following steps:

A  Display the SERDEFL view for the product by entering the following command on the **COMMAND** line:

```
CONtext * product;SERDEFL
```

where *product* is the product name as it appears on the window information line (such as CMF, MVMVS, or MVIP).

B  In the **Member Suffix** field of the SERDEFL view, place the cursor on the suffix that matches the value shown in the **SerDef Suffix** field of TGTDEFD and press **Enter**.

The SERDEFOV view is displayed. SERDEFOV is an overview of the default resource definitions for the specified product.
Using Plex Manager security tracing options

Plex Manager provides a variety of diagnostic tracing options, including one to trace the security calls that are being made by any MainView product.

**NOTE**

In addition to Plex Manager security tracing, you can use the trace facilities and violation reports that are provided by your ESM. Refer to your ESM documentation for information about additional troubleshooting tools.

**To trace security calls for a MainView product**

1. Navigate to the MainView product whose security calls you want to trace.

2. On the **COMMAND** line of any product view, type **DIAGMSG** and press **Enter**.

   The DIAGMSG view is displayed, as shown in **Figure 17**.

**Figure 17  DIAGMSG view**

<table>
<thead>
<tr>
<th>ddmmyyyy hh:mm:ss</th>
<th>COMMAND ===&gt;</th>
<th>SCROLL ===&gt;</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CURR WIN ===&gt; 1</td>
<td>ALT WIN ====&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WI = DIAGMSG======SYSB=======*=========ddmmmyyyy==hh:mm:ss==PLEXMGR==D==11===</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMD Option</td>
<td>Status</td>
<td>Scope</td>
<td>Description / Diagnostic Activity</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>GXDM</td>
<td>OFF</td>
<td>Global</td>
<td>Extended Diagnostic Mode</td>
</tr>
<tr>
<td>LXDM</td>
<td>OFF</td>
<td>Local</td>
<td>Extended Diagnostic Mode</td>
</tr>
<tr>
<td>GEMM</td>
<td>ON</td>
<td>Global</td>
<td>Extended Message Mode</td>
</tr>
<tr>
<td>LEMM</td>
<td>OFF</td>
<td>Local</td>
<td>Extended Message Mode</td>
</tr>
<tr>
<td>LSEMM</td>
<td>OFF</td>
<td>Local</td>
<td>Security Extended Message Mode</td>
</tr>
<tr>
<td>LESTR</td>
<td>OFF</td>
<td>Local</td>
<td>Extended Security Trace</td>
</tr>
<tr>
<td>GESTR</td>
<td>OFF</td>
<td>Global</td>
<td>Extended Security Trace</td>
</tr>
<tr>
<td>LSSTR</td>
<td>OFF</td>
<td>Local</td>
<td>Simple Security Trace</td>
</tr>
<tr>
<td>GSSTR</td>
<td>OFF</td>
<td>Global</td>
<td>Simple Security Trace</td>
</tr>
<tr>
<td>GSSM</td>
<td>OFF</td>
<td>Global</td>
<td>Safe Security Message Display</td>
</tr>
<tr>
<td>WSXASTR</td>
<td>OFF</td>
<td>Window</td>
<td>Extended Authorization Simple Trace</td>
</tr>
</tbody>
</table>

3. In the **CMD** line command field next to WSXASTR, type **ON** and press **Enter**.

   Extended Authorization Simple Trace is enabled. Extended Authorization is the internal process that MainView uses to authorize end-user access to resources that are protected by the security interface. When this diagnostic option is enabled, simple trace messages for Extended Authorization security calls from the current window are displayed prior to the requested view being displayed.
4 On the COMMAND line, type the VIEW command for the view that you want to trace.

A list of security calls (such as RACROUTE calls) is displayed in the current window instead of view data, as shown in Figure 18.

Figure 18  Sample Extended Authorization Simple Trace messages

![Sample Extended Authorization Simple Trace messages](image)

5 After reviewing the security calls, press Enter or END to display the requested view.

**NOTE**

Extended Authorization Simple Trace remains enabled until you turn it off from the DIAGMSG view. A list of security calls will be displayed for each view that you request. To display the view itself, press Enter or END.

---

**Troubleshooting in full-screen mode**

This section describes how to

- verify the status of full-screen mode security
- troubleshoot MainView AutoOPERATOR advanced security
- troubleshoot MainView for CICS security
Verifying the status of full-screen security

This section presents a series of checks that you can perform to verify the overall status of full-screen security.

To verify the status of full-screen security

1. Check the SYSLOG and the BBI journal for any messages that were created during BBI-SS PAS initialization.

   The following message is issued when security through the SAF interface is in use:

   \[
   SM3209I \ \text{SECURITY DEFINITIONS RETRIEVED FROM} \ \text{xxxxxxx ssid}
   \]

   where

   \[
   \text{xxxxxxx} \quad \text{identifies whether security has been turned on from SYS1.PARMLIB,}
   \]

   \[
   \text{the logical PARMLIB concatenation, or the BBIPARM concatenation}
   \]

   \[
   \text{ssid} \quad \text{is the name of the BBI-SS PAS that is secured}
   \]

   Use this message to determine which BBI-SS PAS has had security turned on and from where.

2. Check the syntax of the TYPE=BBI statement in the BBSEC member.

   If message SM3209I did not show up in the SYSLOG or BBI journal during BBI-SS PAS initialization, the syntax of the TYPE=BBI statement in the BBSEC member might be incorrect.

   A. Check the SS parameter to determine whether the correct BBI-SS PAS is being identified.

      Regardless of how many BBSEC members exist in SYS1.PARMLIB, the logical PARMLIB concatenation, and the BBIPARM concatenation, MainView uses the first TYPE=BBI statement where the SS=ssid parameter matches the subsystem ID of the BBI-SS PAS. An unexpected match might occur because of wildcards (such as asterisks) in the SS=ssid parameter.

   B. Check the CLASS and PREFIX parameters to determine whether the correct security class and prefix are being used.

      If the CLASS or PREFIX parameters are not specified correctly, the defaults of CLASS=$BOOLE and PREFIX=BBM are used.
3 If changes were made to a secured resource, ensure that the resource was correctly refreshed within the ESM.

All changes that are made to a user’s security access are dynamic. After a 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.

4 Check the ESM’s audit trail for the resource name and user ID that are being verified.

Because it is possible for a resource to be protected by multiple security profiles when generics are used, you should perform the following tasks:

A Enable any tracing or auditing facilities that the ESM provides.

B Check the output to determine exactly which resource name and user ID are being verified.

5 If changes were made to the BBSEC member, ensure that the BBI-SS PAS was restarted.

All information related to security is obtained from the BBSEC member during BBI-SS PAS initialization. If you make changes to BBSEC, warm start the affected BBI-SS PAS so that the updates take effect.

### Checking MainView AutoOPERATOR advanced security

If you encounter security problems with MainView AutoOPERATOR advanced security, check the following items:

1 Check the SYSLOG or the BBI journal for any of the following messages created during initialization when any MainView 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
AA3221I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=ALRTEXEC IN USE
AA3223I  SECURITY DEFINITIONS FOR TYPE=AAO FEATURE=IMSGEN IN USE
```

Each MainView 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 MainView AutoOPERATOR advanced security CMD feature 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 being 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 CLASS=$BOOLE and CLASS=DATASET:

<table>
<thead>
<tr>
<th>Command</th>
<th>Resource name when CLASS=$BOOLE</th>
<th>Resource name when CLASS=DATASET</th>
</tr>
</thead>
<tbody>
<tr>
<td>/D SLIP=ID01</td>
<td>prefix.ssid.AAO.target.MVSCMD.D.SLIP</td>
<td>prefix.ssid.AAO.target.MVSCMD.D.SLIP</td>
</tr>
<tr>
<td>/DIS A</td>
<td>prefix.ssid.AAO.target.IMSCMD.DIS.A</td>
<td>prefix.ssid.AAO.target.IMSCMD.DIS.A</td>
</tr>
</tbody>
</table>

Note: Commands, parameters, and keywords are truncated at eight characters.

3 When MainView AutoOPERATOR advanced security features are in use, check to see if the correct resource name is defined to the ESM.

When either the CMD or EXEC feature is in use, the more discrete level of checking overrides basic security checks when the command is issued from the terminal session COMMAND line.

The following table shows commands that can be issued and the corresponding resource name that is checked when either CLASS=DATASET or CLASS=$BOOLE is specified:

<table>
<thead>
<tr>
<th>Command</th>
<th>Resource name without advanced security</th>
<th>Resource name with advanced security</th>
</tr>
</thead>
<tbody>
<tr>
<td>/D SLIP=ID01</td>
<td>prefix.ssid.AAO.target.MVSCMD</td>
<td>prefix.ssid.AAO.target.MVSCMD.D.SLIP</td>
</tr>
<tr>
<td>/DIS A</td>
<td>prefix.ssid.AAO.target.IMSCMD</td>
<td>prefix.ssid.AAO.target.IMSCMD.DIS.A</td>
</tr>
<tr>
<td>%TESTEXEC</td>
<td>prefix.ssid.AAO.target.EXEC</td>
<td>prefix.ssid.AAO.target.EXEC.TESTEXEC</td>
</tr>
</tbody>
</table>

Note: Commands, parameters, and keywords are truncated at eight characters.
Checking MainView for CICS security

If you encounter security problems with MainView for CICS, check the following items:

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 might be intervening messages.

2. Check the syntax of the TYPE=CICS statement.

   If the BCO006I message 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 might be incorrect.
Troubleshooting in MainView Explorer

Problems accessing MainView Explorer are often caused by restricted access to host data sets or some other MainView security call on the host server. For example, any of the following situations could prevent a user from being able to access MainView Explorer:

- The user does not have a valid user ID on the system where the MainView Explorer host server address space is running.
- A problem exists with the host server address space (such as a problem connecting to the CAS or a problem with the default port, 3940).
- Some required MainView resource (such as connecting to the CAS) is universally secured.

The JES output for the MainView Explorer host server address space should look something like this example:

```
$HASP373 MV$MXP STARTED
IEF403I MV$MXP - STARTED - TIME=02.29.46
BBTM232I Reading TCP parameters from parmlib member BBTTCP00
BBTM100I BMC Software TCP/IP Interface Initialization in progress
BBTM898I Located TCP/IP Address Space TCPIP (V6.4)
BBTM899I TCP/IP Address Space TCPIP Selected (BBT4LOAD)
BBWIC050I Host Server IP address: 192.168.7.5, PORT: 3940
BBWIC051I TCP/IP server is ready
BBWIA001I Explorer Host Server is starting
BBWIB030I CAS(BBCS) connection is established
BBWIE001I MAINVIEW Explorer (v.r.mm) services are available
BBMXCL36I Default Security Resource Definition BBWTRN used for MVEXP
--- SUNDAY, 11 JAN 2004 ----
BBWIC054I Session started for 172.23.134.75
```
Case study: MainView for DB2

This appendix presents a detailed example of the security that could be defined for the following site:

<table>
<thead>
<tr>
<th>Product Installed</th>
<th>MainView for DB2 (windows and full-screen mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Environment</td>
<td>multiple LPARs and databases, divided into production and test environments</td>
</tr>
<tr>
<td>User Groups</td>
<td>Technical Services (system programmers and DBAs)</td>
</tr>
<tr>
<td></td>
<td>Operations</td>
</tr>
<tr>
<td></td>
<td>Production Staff</td>
</tr>
<tr>
<td></td>
<td>Development DBAs</td>
</tr>
<tr>
<td></td>
<td>Application Programmers (Levels 1 and 2)</td>
</tr>
<tr>
<td>ESM Being Used</td>
<td>CA ACF2</td>
</tr>
</tbody>
</table>

Windows-mode security

For windows-mode security, the following parameters are used:

<table>
<thead>
<tr>
<th>ESMTYPE(AUTO)</th>
<th>MainView automatically determines which ESM is installed and active.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASS('$BBM') NEXT - 'MAINVIEW'</td>
<td>The default security class of $BBM is transformed to class MainView by use of a NEXT statement.</td>
</tr>
</tbody>
</table>
To protect MainView for DB2 windows-mode resources, the site grants the following access:

- The Technical Services staff has access to all product data and actions on all DB2 systems.
- All other users have read-only access to product data.
- Some users are prevented from accessing certain DB2 systems (for example, the Production Staff is denied access to test systems).

To define this security environment, the site uses CA ACF2 rules as shown in Figure 19.

**Figure 19 Sample CA ACF2 rules for MainView for DB2, windows mode (part 1 of 2)**

```
$KEY(MVDB2) TYPE(MVW)
$PREFIX(BBM)

* TECHNICAL SERVICES ACCESS (1ST LEVEL)

- MVDB2.- UID(sysprog) ALLOW
- MVDB2.- UID(techdba) ALLOW
- MVDB2.- UID(-) PREVENT

* OPERATIONS STAFF ACCESS (1ST LEVEL) ALL DB2

- MVDB2.- UID(operator) ALLOW

* PRODUCTION STAFF ACCESS (1ST LEVEL) ALL DB2 BUT TEST

- MVDB2.- UID(prodexpl) ALLOW
SYSD.MVDB2.- UID(prodexpl) PREVENT
SJSĐ.MVDB2.- UID(prodexpl) PREVENT
```
Figure 19  Sample CA ACF2 rules for MainView for DB2, windows mode (part 2 of 2)

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Access</th>
<th>User ID</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBA/DEV (1ST LEVEL)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYSA.MVDB2.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>SYSC.MVDB2.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>SYSE.MVDB2.DB2M.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>SYSE.MVDB2.DB2C.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>SYSH.MVDB2.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>SYSJ.MVDB2.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>SYST.MVDB2.DB1S.</td>
<td>ALLOW</td>
<td>devdba</td>
<td></td>
</tr>
<tr>
<td>APPLICATION 1 (1ST LEVEL)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYSP.MVDB2.</td>
<td>ALLOW</td>
<td>appl1</td>
<td></td>
</tr>
<tr>
<td>SYSP.MVDB2.</td>
<td>ALLOW</td>
<td>appl2</td>
<td></td>
</tr>
<tr>
<td>APPLICATION 2 (1ST LEVEL)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYST.MVDB2.DB2V.</td>
<td>ALLOW</td>
<td>appl2</td>
<td></td>
</tr>
<tr>
<td>SYSE.MVDB2.DB2W.</td>
<td>ALLOW</td>
<td>appl2</td>
<td></td>
</tr>
<tr>
<td>VIEWS ACCESS (2ND LEVEL) FOR TECHNICAL SERVICES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALL ACCESS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVDB2.</td>
<td>ALLOW</td>
<td>sysprog</td>
<td></td>
</tr>
<tr>
<td>MVDB2.</td>
<td>ALLOW</td>
<td>techdba</td>
<td></td>
</tr>
<tr>
<td>VIEWS ACCESS (2ND LEVEL) FOR EVERY BODY ELSE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BROWSE ACCESS (OD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVDB2.</td>
<td>PREVENT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVDB2.</td>
<td>ALLOW</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Full-screen mode security

For full-screen mode security, a common BBSEC member is created for all LPARs where MainView for DB2 is running. The BBSEC member contains the following TYPE statements:

```
TYPE=BBI,SSID=M2*,PREFIX=FSDB2,CLASS=MAINVIEW
TYPE=DB2,SSID=M2*
```

At this site, the naming convention for BBI-SS PAS subsystem IDs is M2&SYSCON. They have chosen a resource name prefix of FSDB2 and a security class name of MainView.

**NOTE**

The security class called MainView must be defined to CA ACF2.

To protect MainView for DB2 full-screen mode resources, the site uses CA ACF2 rules as shown in Figure 20 on page 97.
**Figure 20  Sample CA ACF2 rules for MainView for DB2, full-screen mode (part 1 of 2)**

```
* MAINVIEW RULES FOR FULL-SCREEN MODE FOR MAINVIEW FOR DB2
* FORMAT........FSDB2.M2D0.BBI.DB2Z.ACCESS
* FORMAT....FSDB2.M2-.BBI.DB-.PMACC# (MODIFY ANALYZER/MONITOR)
* FSDB2.M2-.BBI.DB-.BBICMD (MAINVIEW COMMAND)
* FSDB2.M2-.BBI.DB-.BBIJRNL (MAINVIEW JOURNAL)
* FSDB2.M2-.BBI.DB-.DB2CMD (DB2 COMMAND)
* FSDB2.M2-.DMR.DB-.DB2SQL- (DISPLAY SQL TEXT IN TRACE)

$KEY(FSDB2) TYPE(MVW)

* appl1    = APPLICATION 1
* appl2    = APPLICATION 2
* devdba   = DEV DBA
* operator = OPERATIONS STAFF
* prodexpl = PROD/EXPLOITATION STAFF

* TECHNICAL SERVICES ALL ACCESS

- UID(sysprog) ALLOW
- UID(techdba) ALLOW
- UID(-) PREVENT

* OPERATIONS STAFF ACCESS ALL DB2

M2-.BBI.-.ACCESS UID(operator) ALLOW
M2-.BBI.-.PMACCA UID(operator) ALLOW
M2-.DMR.-.DB2SQL- UID(operator) ALLOW

* PRODUCTION STAFF ACCESS ALL DB2 BUT TEST

M2D*.BBI.-.ACCESS UID(prodexpl) PREVENT
M2-.BBI.-.ACCESS UID(prodexpl) ALLOW
M2-.BBI.-.PMACCA UID(prodexpl) ALLOW
M2-.DMR.-.DB2SQL- UID(prodexpl) ALLOW

* DEV DBA 1ER LEVEL - ACCESS BY ENVIRONNEMENT

M2A1.BBI.-.ACCESS UID(devdba) ALLOW
M2C1.BBI.-.ACCESS UID(devdba) ALLOW
M2E1.BBI.DB2C.ACCESS UID(devdba) ALLOW
M2E1.BBI.DB2M.ACCESS UID(devdba) ALLOW
M2H1.BBI.-.ACCESS UID(devdba) ALLOW
M2J1.BBI.-.ACCESS UID(devdba) ALLOW
M2T1.BBI.DB1S.ACCESS UID(devdba) ALLOW

* DEV DBA 2ND LEVEL - SPECIFIC ACTION PERMITTED

M2-.BBI.-.PMACCA UID(devdba) ALLOW
M2-.DMR.-.DB2SQL- UID(devdba) ALLOW
```
**Figure 20  Sample CA ACF2 rules for MainView for DB2, full-screen mode (part 2 of 2)**

```
M2C1.BBI.-.TRACE.-   UID(devdba) LOG
M2C1.BBI.-.TRALLOC-  UID(devdba) LOG
M2E1.BBI.DB2C.TRACE.- UID(devdba) LOG
M2E1.BBI.DB2C.TRALLOC- UID(devdba) LOG

M2P1.BBI.-.ACCESS    UID(********appl1) ALLOW
M2P1.BBI.-.PMACCA    UID(********appl1) ALLOW
M2P1.DMR.-.DB2SQL-   UID(********appl1) ALLOW
M2P1.BBI.-.TRACE.-   UID(********appl1) LOG
M2P1.BBI.-.TRALLOC-  UID(********appl1) LOG

M2T1.BBI.DB2V.ACCESS  UID(********appl2) ALLOW
M2E1.BBI.DB2W.ACCESS  UID(********appl2) ALLOW
M2-.BBI.-.PMACCA     UID(********appl2) ALLOW
M2-.DMR.-.DB2SQL-    UID(********appl2) ALLOW
M2E1.BBI.DB2W.TRACE.- UID(********appl2) LOG
M2E1.BBI.DB2W.TRALLOC- UID(********appl2) LOG
```
Index

Symbols

$BBM security class
  changing 47
description 45
$BOOLE security class 49
$USERID member 59

A

access requirements
  MainView Alarm Management 22
  MainView common registry 22
  superuser authority 22
ACCESS resource 66
access, controlling
  BBI control commands 75
  BBSEC member 79
  CAS 64
  DB2 commands 75
  MainView Alternate Access 75
  MVS commands 75
  PAS 66
  Plex Manager resources 78
  product actions 71
  product data 67
  security resources 78
  target system 66
actions, controlling access to
  full-screen mode 73
  windows mode 72
authorized command table, updating 27
authorizing CAS and PAS
  CA ACF2 26
  CA Top Secret 31
  RACF 23

B

B1 security requirements 16, 38
basic security. See full-screen mode security
BBI control commands, access to 75
BBIJNT00 member 58
BBMTSP00 member 48
BBMTSS00 member
defining security parameters 39
disabling security 61
BBPARM data set
  $USERID member 59
  BBIJNT00 member 58
  BBSEC member 41, 43
BBSAMP data set 59
BBSEC member
controlling access 79
creating 41
description 19
disabling security 62
sample 44
TYPE statement 41
BBSECURE data set
  BBMTSP00 member 48
  BBMTSS00 member 39, 61
description 16
  windows-mode security 82
BMC Software, contacting 2

C

CA ACF2
  adding SAF resource class 28
  authorizing CAS and PAS 26
  case study 93
  customizing GSO record options 25
  defining $BOOLE security class 50
  overview of setup (windows mode) 25
  sample rules 94, 97
  securing CASs 65
  securing MainView Alternate Access 76
  securing product actions 75
  securing product data 69, 71
  securing target systems 67
  updating authorized command table 27
  updating SAFDEF list 26
CA Top Secret
  adding SAF resource class 32
  authorizing CAS and PAS 31
  defining $BOOLE security class 50
  defining facility matrix entry 30
  defining resource ownership 33
CA Top Secret (continued)
  overview of setup (windows mode) 30
  securing CASs 65
  securing MainView Alternate Access 76
  securing product actions 75
  securing product data 69, 71
  securing target systems 67
CAS. See coordinating address space (CAS)
CASDEFD view 83, 84

case study, MainView for DB2
  full-screen mode 96
  windows mode 93

CLISTs, resource
  MainView AutoOPERATOR 60
  MainView for CICS 60
  MainView for DB2 60
  MIGUSER 59
  RACFDEF 59
  using 59

coordinating address space (CAS)
  authorizing 23, 26, 31
  controlling access 64
  identifying security members 82
  resource name 64

customer support 3


data, controlling access to
  full-screen mode 70
  windows mode 68

DB2 commands, access to 75
DIAGMSG view 86

disabling resource definitions 56

disabling security
  full-screen mode 62
documentation, related 12

electronic documentation 11

enabling resource definitions 56

enhanced security. See windows-mode security

ESM setup (windows mode)
  CA Top Secret 30
  RACF 23

ESM, identifying to MainView
  BBMTSS00 member 40
  SEPDEF views 38

ESMGRINH statement 40

ESMTYPE statement
  disabling security 61
  identifying ESM 40

Extended Authorization Simple Trace 86

EZPLEX menu 17

EZSEC menu 16

F

facility matrix entry, defining 30

FACILITY security class 45

full-screen mode security
  ACCESS resource 66
  BBSEC member 19
  disabling 62
  overview 19
  PAS access 66
  products that use 19
  resource CLISTs 59
  resource names 57
  security class 49
  security parameters 41
  security resources, protecting 79
  status, checking 88
  target system access 66
  troubleshooting 87

G

GROUP Inherit, setting
  BBMTSS00 member 40
  SEPDEF views 38

GSO record options, customizing 25

H

Help, online 11

M

MainView Alternate Access 75
MainView AutoOPERATOR
  access to MVS commands 75
  FEATURE keyword 43
  resource CLISTs 60
  troubleshooting 89
  TYPE statement 42

MainView Explorer 92

MainView for CICS
  access to product actions 74
  resource CLIST 60
  troubleshooting 91
  TYPE statement 42

MainView for DB2
  access to DB2 commands 75
  case study 93
  command-level security 43
  resource CLISTs 60
  TYPE statement 42
MainView for z/OS
- access to SYSPROG Services 75
- MVScope data 73
MainView products, security for 19
MainView security interface 15
MainView Selection Menu 17
MainView session, starting 16
MainView SYSPROG Services
  - access to action services 75
    - BBSEC location 41
    - TYPE statement 42
  MIGUSER CLIST 59
  MVScope commands, access to 75
  MVScope data, access to 73

N
NEXT parameter 45, 48

O
online Help 11

P
PAS. See product address space (PAS)
Plex Manager
  - accessing 17
  - resource definitions 54
  - security resources, protecting 78
  - tracing options 86
product actions, controlling access to
  - full-screen mode 73
  - windows mode 72
product address space (PAS)
  - authorizing 23, 26, 31
  - controlling access 66
  - identifying security members 84
product data, controlling access to
  - full-screen mode 70
  - windows mode 68
product support 3
publications, related 12

R
RACF
  - adding SAF resource class 24
  - authorizing CAS and PAS 23
  - defining $BOOLE security class 49
  - generic profiles 50
  - GROUP feature 38, 40
  - overview of setup (windows mode) 23
  - securing CASs 65

RACF (continued)
  - securing MainView Alternate Access 76
  - securing product actions 75
  - securing product data 69, 71
  - securing target systems 67
RACFDEF CLIST 59
RACROUTE calls, displaying 87
related publications 12
resource CLISTS
  - MainView AutoOPERATOR 60
  - MainView for CICS 60
  - MainView for DB2 60
  - MIGUSER 59
  - RACFDEF 59
  - using 59
resource definitions
  - changing 54
  - common 54
  - default 53
  - disabling 56
  - enabling 56
  - Plex Manager 54
resource names
  - CAS 64
  - full-screen mode 57, 58
  - windows mode 51
resource ownership, defining to CA Top Secret 33

S
SAF resource class, adding
  - CA ACF2 28
  - CA Top Secret 32
  - RACF 24
SAFDEF list, updating 26
SECDEF view 46
SECDEFL view 46
security class
  - $BBM 45, 47
  - $BOOLE 49
  - FACILITY 45
  - full-screen mode 49
  - windows mode 45
security parameters
  - BBMTSS00 member 39
  - full-screen mode 41
  - SEPDEF views 36
  - windows mode 36
security resources, protecting
  - full-screen mode 79
  - Plex Manager 78
  - windows mode 78
security tracing, Plex Manager 86
security views
SECDEF 46
SECDEFL 46
SEPDEFL 37
SERDEFEX 55
SERDEFL 54
SERDEFOV 55
SEPDEFL view 37
SERDEFEX view 55
SERDEFL view 54
SERDEFOV view 55
starting MainView 16
superuser authority requirements 22
support, customer 3

T
technical support 3
TGTDEFD view 85
tracing, security 86
troubleshooting
  full-screen mode 87
  MainView Explorer 92
  windows mode 82
TYPE statement 41

V
views
  CASDEFD 83, 84
  DIAGMSG 86
  SECDEF 46
  SECDEFL 46
  SEPDEFL 37
  SERDEFEX 55
  SERDEFL 54
  SERDEFOV 55
  TGTDEFD 85

W
windows-mode security
  BBMTSP00 member 48
  BBMTSS00 member 39, 61
  BBSECURE data set 16, 82
  changing resource definitions 54
  common resources 54
  disabling resource definitions 56
  enabling resource definitions 56
  EZSEC menu 16
  overview 16
  products that use 19
  resource names 51
  SECDEF views 45
  security class 45
  security parameters 36
  security resources, protecting 78
  SEPDEF views 36
  SERDEF views 54
  troubleshooting 82
  W$XASTR option 86