Contents

Overview of customizing BMC system administration products for IMS .......... 9
BMC system administration products and components for IMS ............... 10

Customizing BMC Log Analyzer for IMS ........................................... 11
Overview of customizing BMC Log Analyzer for IMS ............................ 11
BMC Log Analyzer for IMS customization worksheet ............................ 11
Completing BMC Log Analyzer for IMS customization .......................... 12
  To customize the interface ......................................................... 12

Customizing BMC System Administration for IMS ............................... 13
Overview of customizing BMC Administration for IMS products ............. 13
BMC System Administration for IMS customization worksheet ............... 14
Completing BMC System Administration for IMS customization ............. 15

Customizing BMC System Communication for IMS ............................... 16
Overview of customizing BMC System Communication for IMS ............... 17
BMC System Communication for IMS customization worksheet ............... 17
Completing BMC System Communication for IMS customization ............. 18

Customizing DELTA IMS and DELTA IMS VIRTUAL TERMINAL .......... 19
Overview of customizing DELTA IMS and DELTA IMS VIRTUAL TERMINAL . . 19
  DELTA IMS customization worksheet .......................................... 20
  Updating IMS ............................................................................ 20
  Updating MVS for APPC support .................................................. 23
    To update MVS for APPC support .............................................. 23
  Updating VTAM ........................................................................ 24
  Adding DELTA IMS to TSO/ISPF .................................................. 26
    Accessing DELTA IMS from a CLIST ............................................ 26
    Accessing DELTA IMS from an ISPF options menu ....................... 27
    Setting DELTA IMS default ISPF values .................................... 28
  Limiting access to DELTA IMS ..................................................... 30
    Implementing user access profiles ............................................. 31
  Setting global options .................................................................. 37
    To set global options .............................................................. 37
  Setting IMSID options .................................................................. 42
    To create a new IMSID ............................................................ 42
Creating and formatting Log and History File data sets ........................................... 88
  To create and format the Log data set ................................................................. 88
  To create and format the History File data set ..................................................... 89
Creating View Profiles ............................................................................................... 90
  Using DELTA PLUS defaults .................................................................................. 90
  Using an existing View Profile .............................................................................. 91
  Using a conversion utility ....................................................................................... 91
  Available commands ............................................................................................. 91
Editing View Profiles .................................................................................................. 96
  To edit a View Profile ............................................................................................ 97
  To create a new View Profile ................................................................................ 103
Allocating new data sets ............................................................................................ 104
  To allocate a new data set ..................................................................................... 104
Adding an IMSID to an existing Group's Log data sets ............................................. 107
  To add an IMSID to an existing Group's Log data sets ....................................... 107
  To add the IMSID to the specified Group's Log and History File data sets later .... 108
Completing DELTA PLUS VIRTUAL TERMINAL customization ......................... 109
  Enabling DELTA PLUS VIRTUAL TERMINAL ............................................... 109
  Setting virtual terminal IMSID options ................................................................ 109
  Refreshing TSS tables ............................................................................................ 126
Starting products ........................................................................................................ 127
  To start the products ............................................................................................. 127
DELTA PLUS VIRTUAL TERMINAL customization worksheet ......................... 127

Customizing Energizer for IMS Connect ................................................................. 129
Overview of customizing Energizer for IMS Connect ............................................. 129
Energizer for IMS Connect customization worksheet ............................................. 129
Adding Energizer to TSO/ISPF ............................................................................... 130
  Accessing Energizer from a CLIST ...................................................................... 130
  Accessing Energizer from an ISPF options menu .............................................. 130
  Using the Energizer ISPF interface .................................................................... 132
Completing Energizer implementation .................................................................... 134
Adding BMC security ............................................................................................... 136
Archiving journal data sets automatically ............................................................... 137
  To archive journal data sets automatically ......................................................... 137

Customizing EXTENDED TERMINAL ASSIST PLUS .......................................... 138
Overview of customizing Extended Terminal Assist Plus .......... 138
EXTENDED TERMINAL ASSIST PLUS customization worksheet .... 139
Running ETA without ETO ............................................. 139
  To discontinue using ETO with ETA ........................... 140
  To configure ETA to run without ETO ......................... 141
Updating VTAM (ETA) ................................................... 141
Adding ETA to TSO/ISPF ............................................. 143
  Accessing ETA from a CLIST .................................... 143
  Accessing ETA from an ISPF options menu ................. 144
Limiting access to ETA .................................................. 145
  Implementing user access profiles and UPF security1 .... 147
  Implementing a SAF interface to RACF (or equivalent) product1 150
Setting global options in ETA ........................................ 153
  To set global options ........................................... 154
Setting IMSID options for ETA ...................................... 156
  To set IMSID options ........................................... 157
Setting TSS IMSID options ......................................... 160
Setting Group options for ETA ..................................... 162
  To set Group options ........................................... 163
Starting ETA ............................................................. 164
Customizing LOCAL COPY PLUS ...................................... 165
Overview of customizing Local Copy Plus ......................... 165
LOCAL COPY PLUS customization worksheet ...................... 166
Adding LOCAL COPY PLUS to TSO/ISPF ......................... 166
  Accessing LOCAL COPY PLUS from a CLIST ................. 167
  Accessing LOCAL COPY PLUS from an ISPF options menu ... 167
  Setting LOCAL COPY PLUS default ISPF values .......... 168
  Setting LOCAL COPY PLUS default ISPF IMSID values ...... 170
Limiting access to LOCAL COPY PLUS ............................. 172
  Implementing an internally coded list ........................ 173
  Implementing ACF2 ................................................ 175
  Implementing RACF ............................................... 176
Setting LOCAL COPY PLUS options ............................... 177
  Setting LOCAL COPY PLUS IMSID options ................. 177
Specifying LOCAL COPY PLUS Destination Entries ............. 178
  Setting LOCAL COPY PLUS Copy Table Entry options ...... 178
Customizing Message Advisor for IMS ............................................. 179
Overview of customizing Message advisor for IMS .......................... 179
Message Advisor customization worksheet ..................................... 179
Adding Message Advisor to TSO/ISPF ........................................ 181
  Accessing Message Advisor from a CLIST ................................. 181
  Accessing Message Advisor from an ISPF options menu ............... 181
  Allocating a request library for Message Advisor ....................... 183
Limiting access to Message Advisor ........................................... 184
  Implementing an internally coded list (function,userid,imsid,subfunction
  authorization) ................................................................. 185
  Implementing a SAF product ................................................ 188
  Implementing an ACF2 product .............................................. 189
Allocating Message Advisor data sets ....................................... 190
  To allocate the data sets that are required for Message Advisor processing 192
Setting the Message Advisor options ........................................ 193
  To set the Message Advisor options ..................................... 198
Setting the Message Advisor QPF options ................................ 200
  To set the Message Advisor QPF options ............................... 200
Adding VTAM parameters ...................................................... 201
  Adding VTAM parameters for a single-CPU environment ............ 202
  Adding VTAM parameters for a multiple-CPU environment ........ 204
Installing the QPF Test Applications ....................................... 210
  To install the QPF Test Applications in your IMS test environment: 210
Installing the Message Advisor Server ..................................... 212
Bringing up your IMS system .................................................. 212
Verifying Message Advisor installation .................................... 213
  Performing the batch IVP for Message Advisor ...................... 214
  Performing the online IVP for Message Advisor .................... 219
  Performing the IVP for QPF ............................................. 223
Customizing the console ............................................................. 227
Overview of customizing the GUI Console .................................. 227
Console customization worksheet .............................................. 227
Customizing the UIM server console ....................................... 228
  Installing the console ..................................................... 228
  Updating the console ...................................................... 229
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstalling the console</td>
<td>229</td>
</tr>
<tr>
<td>Launching and exiting the console</td>
<td>229</td>
</tr>
<tr>
<td>To launch the console</td>
<td>230</td>
</tr>
<tr>
<td>To exit the console</td>
<td>230</td>
</tr>
<tr>
<td>Managing UIM server clients</td>
<td>230</td>
</tr>
<tr>
<td>To manage the UIM server clients</td>
<td>231</td>
</tr>
<tr>
<td>Setting up connections</td>
<td>231</td>
</tr>
<tr>
<td>Overview of the Enterprise List and personal connections</td>
<td>231</td>
</tr>
<tr>
<td>Managing the Enterprise List</td>
<td>232</td>
</tr>
<tr>
<td>Using the Add Host Connection command</td>
<td>232</td>
</tr>
<tr>
<td>Operating the UIM server</td>
<td>234</td>
</tr>
<tr>
<td>Overview of customizing the UIM server</td>
<td>234</td>
</tr>
<tr>
<td>Operating the UIM server1</td>
<td>234</td>
</tr>
<tr>
<td>Starting and stopping the UIM server</td>
<td>234</td>
</tr>
<tr>
<td>Verifying that the UIM server is running</td>
<td>235</td>
</tr>
<tr>
<td>Accessing the BMC UIM server Commands web page</td>
<td>235</td>
</tr>
<tr>
<td>Viewing active users</td>
<td>237</td>
</tr>
<tr>
<td>Changing the security authorization timeout feature temporarily</td>
<td>237</td>
</tr>
<tr>
<td>Enabling or disabling the overall tracing option temporarily</td>
<td>238</td>
</tr>
<tr>
<td>Enabling or disabling specific tracing options temporarily</td>
<td>238</td>
</tr>
<tr>
<td>Refreshing the UIM server content</td>
<td>239</td>
</tr>
<tr>
<td>Merging multiple products into a single UIM server</td>
<td>240</td>
</tr>
<tr>
<td>Sharing a Installation System server with DB2 and IMS products</td>
<td>240</td>
</tr>
<tr>
<td>Sharing UIM server with multiple IMS products</td>
<td>243</td>
</tr>
<tr>
<td>Creating a new UIM server</td>
<td>244</td>
</tr>
<tr>
<td>Creating a startup configuration member</td>
<td>244</td>
</tr>
<tr>
<td>Creating a started task procedure</td>
<td>245</td>
</tr>
<tr>
<td>Setting up the HFS data set</td>
<td>247</td>
</tr>
<tr>
<td>Customizing the UIM server</td>
<td>249</td>
</tr>
<tr>
<td>Changing the port number</td>
<td>250</td>
</tr>
<tr>
<td>Changing the security authorization timeout feature permanently</td>
<td>251</td>
</tr>
<tr>
<td>Changing the idle timeout for affinity tasks</td>
<td>252</td>
</tr>
<tr>
<td>Changing the HFS server-side storage data set name</td>
<td>252</td>
</tr>
<tr>
<td>Enabling or disabling the network browser command interface</td>
<td>253</td>
</tr>
<tr>
<td>Enabling or disabling the overall tracing option permanently</td>
<td>254</td>
</tr>
<tr>
<td>Enabling or disabling specific tracing options permanently</td>
<td>255</td>
</tr>
</tbody>
</table>
Enabling and disabling password caching ........................................... 257

**Operating subsystems and product servers** ....................................... 258
Overview of customizing BMC System Administration for IMS ............ 258
Operating the BMCP subsystem ............................................................ 259
  Started task procedure name for BMCP ............................................ 259
  BMCP subsystem commands ............................................................ 259
Operating the BCSS/CPC subsystem ...................................................... 260
  Started task procedure name for BCSS/CPC .................................. 260
  BCSS/CPC installation .................................................................... 261
  CPC components ................................................................................. 261
  JCL requirements .............................................................................. 262
  BCSS/CPC subsystem commands ....................................................... 262
Operating the IPT server ..................................................................... 263
  Started task procedure name for IPT .............................................. 263
  Security ............................................................................................ 264
  Sysplex implementation .................................................................. 264
  IPT server commands ...................................................................... 265
  CPCINI keywords ............................................................................ 267

**Index** ..................................................................................................... 270
This online document explains how to customize the System Administration Products for IMS after installation.

**December 2015**

**Supporting**

- Version 1.5 of BMC Log Analyzer for IMS
- Version 2.7 of BMC System Administration for IMS
- Version 1.4 of BMC System Communication for IMS
- Version 6.8 of DELTA IMS DB/DC
- Version 6.8 of DELTA IMS DC
- Version 6.8 of DELTA IMS for DBCTL
- Version 2.6 of DELTA PLUS
- Version 2.6 of DELTA PLUS for DBCTL
- Version 2.6 of DELTA PLUS VIRTUAL TERMINAL
- Version 1.7 of Energizer for IMS Connect
- Version 3.6 of EXTENDED TERMINAL ASSIST PLUS
- Version 3.9 of LOCAL COPY PLUS
- Version 1.7 of Message Advisor for IMS

**Overview of customizing BMC system administration products for IMS**

*Customization* refers to tasks that you perform outside the Installation System, *after* you have installed and configured the product libraries.

For information about installation and configuration, see the Installation System documentation.

For information about installing and customizing the product libraries, see the the Installation System documentation.

Product customization can include tasks such as the following:

- Updating IMS
• Updating VTAM
• Providing access to the ISPF interface
• Accessing products from a CLIST
• Accessing products from an ISPF options menu
• Limiting access
• Managing the SAF interface to RACF (or equivalent) product
• Managing user access profiles
• Setting global options
• Setting IMSID options

• BMC system administration products and components for IMS (see page 10)

BMC system administration products and components for IMS

This following table lists the BMC system administration products and components for IMS and specifies where to find configuration or operating information about each one.

<table>
<thead>
<tr>
<th>Product or component</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC Log Analyzer for IMS</td>
<td>Customizing BMC Log Analyzer for IMS (see page 11)</td>
</tr>
<tr>
<td>BMC System Administration for IMS</td>
<td>Customizing BMC System Administration for IMS (see page 13)</td>
</tr>
<tr>
<td>BMC System Communication for IMS</td>
<td>Customizing BMC System Communication for IMS (see page 16)</td>
</tr>
<tr>
<td>DELTA IMS</td>
<td>Customizing DELTA IMS and DELTA IMS VIRTUAL TERMINAL (see page 19)</td>
</tr>
<tr>
<td>DELTA IMS DB/DC</td>
<td></td>
</tr>
<tr>
<td>DELTA IMS DC</td>
<td></td>
</tr>
<tr>
<td>DELTA IMS for DBCTL</td>
<td></td>
</tr>
<tr>
<td>DELTA IMS VIRTUAL TERMINAL</td>
<td></td>
</tr>
<tr>
<td>DELTA PLUS</td>
<td>Customizing DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 52)</td>
</tr>
<tr>
<td>DELTA PLUS for DBCTL</td>
<td></td>
</tr>
<tr>
<td>DELTA PLUS VIRTUAL TERMINAL</td>
<td></td>
</tr>
<tr>
<td>Energizer for IMS Connect</td>
<td>Customizing Energizer for IMS Connect (see page 129)</td>
</tr>
<tr>
<td>EXTENDED TERMINAL ASSIST PLUS</td>
<td>Customizing EXTENDED TERMINAL ASSIST PLUS (see page 138)</td>
</tr>
<tr>
<td>LOCAL COPY PLUS</td>
<td>Customizing LOCAL COPY PLUS (see page 165)</td>
</tr>
</tbody>
</table>
Customizing BMC Log Analyzer for IMS

This section describes customization tasks that are unique to BMC Log Analyzer for IMS. Customizing refers to tasks that you perform outside of the Installation System to complete product implementation. The following Topics are covered:

- Overview of customizing BMC Log Analyzer for IMS (see page 11)
- BMC Log Analyzer for IMS customization worksheet (see page 11)
- Completing BMC Log Analyzer for IMS customization (see page 12)

Overview of customizing BMC Log Analyzer for IMS

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and configuring the product libraries, see the the Installation System documentation.

The customization tasks that are presented are unique to BMC Log Analyzer for IMS.

BMC Log Analyzer for IMS customization worksheet

Refer to the following worksheet as you work through the customization process for BMC Log Analyzer for IMS.

<table>
<thead>
<tr>
<th>Product or component</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Advisor for IMS</td>
<td>Customizing Message Advisor for IMS (see page 179)</td>
</tr>
<tr>
<td>UIM server and the console</td>
<td>• Customizing the console (see page 227)</td>
</tr>
<tr>
<td></td>
<td>• Operating the UIM server (see page 234)</td>
</tr>
<tr>
<td>Subsystems and product servers</td>
<td>Operating subsystems and product servers (see page 258)</td>
</tr>
</tbody>
</table>
### Completing BMC Log Analyzer for IMS customization

This section describes the steps for customizing BMC Log Analyzer for IMS.

To customize BMC Log Analyzer for IMS, you must customize the Log Analyzer ISPF interface. Log Analyzer includes a sample CLIST that you can use to invoke the ISPF interface. This CLIST provides dynamic access to Log Analyzer libraries (through LIBDEF instructions) and displays the main menu of the Log Analyzer ISPF interface. You must customize the CLIST to point to the installed Log Analyzer libraries. You can also preset ISPF profile variables for the interface.

#### To customize the interface

1. Copy member LUICI@00 of the SAMP library to your system CLIST library.
2. Edit member LUICI@00.
   a. Change all instances of `BMCNODE` to the high-level qualifier `<hlq>` that was used to allocate the Log Analyzer libraries.
   
   The `<hlq>` is your user ID unless you changed the value of the PROFILE keyword in the job that expanded the installation image.
   b. Change all instances of `prd` to the appropriate value based on whether you chose merged libraries or non-merged libraries during installation.
   c. Save the changes to member LUICI@00.

#### Note

For more information about merged and non-merged libraries, see the Installation System documentation.

- If you chose merged libraries, change `prd` to `IM`.
- If you chose non-merged libraries, change `prd` to `LUI`.

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Copy member LUICI@00 to your system CLIST library.</td>
<td>Completing BMC Log Analyzer for IMS customization (see page 12)</td>
</tr>
<tr>
<td>2.</td>
<td>Edit member LUICI@00.</td>
<td>Completing BMC Log Analyzer for IMS customization (see page 12)</td>
</tr>
<tr>
<td>3.</td>
<td><em>(optional)</em> Preset profile variables.</td>
<td>Completing BMC Log Analyzer for IMS customization (see page 12)</td>
</tr>
<tr>
<td>4.</td>
<td>Test the CLIST.</td>
<td>Completing BMC Log Analyzer for IMS customization (see page 12)</td>
</tr>
</tbody>
</table>
3. *(optional)* Preset profile variables.
   You can preset profile variables for all users of the interface. Edit member LUIZUSER of the
   PLIB library as explained in the comments.

4. Test the CLIST by entering the following command on any ISPF panel that accepts TSO
   commands:
   
   **TSO %LUICI@00**
   
   The Log Analyzer logo panel is displayed. When you press *Enter*, the Log Analyzer Main
   Menu is displayed.

---

**Customizing BMC System Administration for IMS**

The customization tasks are unique to BMC System Administration *for IMS*. *Customizing* refers to
tasks that you perform outside of the Installation System to complete product implementation. The
following topics are covered in this section:

- Overview of customizing BMC Administration for IMS products (see page 13)
- BMC System Administration for IMS customization worksheet (see page 14)
- Completing BMC System Administration for IMS customization (see page 15)

---

**Overview of customizing BMC Administration for IMS products**

You should complete the customization tasks after you have installed and configured the product
libraries through the Installation System.

For information about installing and configuring the product libraries, see the Installation System
documentation.

---

**Note**

No configuration tasks were performed for the following BMC products for IMS:

- DELTA PLUS
- DELTA PLUS VIRTUAL TERMINAL
- EXTENDED TERMINAL ASSIST PLUS
- Message Advisor *for IMS*

The customization tasks are unique to BMC System Administration *for IMS*. 
Depending on the products that you are installing as part of this solution, you might also need to complete customization tasks that are applicable to the following BMC system administration products for IMS:

<table>
<thead>
<tr>
<th>Product</th>
<th>Location of configuration tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC Log Analyzer for IMS</td>
<td>Customizing BMC Log Analyzer for IMS (see page 11)</td>
</tr>
<tr>
<td>DELTA PLUS</td>
<td>Customizing DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 52)</td>
</tr>
<tr>
<td>DELTA PLUS VIRTUAL TERMINAL</td>
<td>Customizing DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 52)</td>
</tr>
<tr>
<td>Energizer for IMS Connect</td>
<td>Customizing Energizer for IMS Connect (see page 129)</td>
</tr>
<tr>
<td>EXTENDED TERMINAL ASSIST PLUS (ETA)</td>
<td>Customizing EXTENDED TERMINAL ASSIST PLUS (see page 138)</td>
</tr>
<tr>
<td>Message Advisor for IMS</td>
<td>Customizing Message Advisor for IMS (see page 179)</td>
</tr>
</tbody>
</table>

**BMC System Administration for IMS customization worksheet**

Refer to the following worksheet as you work through the customization process for BMC System Administration for IMS:

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Ensure that the common library is APF-authorized.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
<tr>
<td></td>
<td>2. Install and configure the BMCP subsystem.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
<tr>
<td></td>
<td>3. Assemble and link the CPCOPT macro into the IPTLIB library.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
<tr>
<td></td>
<td>4. Copy the required members from IPTSAMP to your SYSx PROCLIB.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
<tr>
<td></td>
<td>5. Customize the Log Analyzer ISPF interface.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
<tr>
<td></td>
<td>6. Start the UIM server.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
<tr>
<td></td>
<td>7. Install the console.</td>
<td>Completing BMC System Administration for IMS customization</td>
</tr>
</tbody>
</table>
Completing BMC System Administration for IMS customization

This section describes customizing BMC System Administration for IMS.

1. Ensure that the common load library that contains code for all products is APF-authorized before starting any of the newly-created started tasks.
2. Install and configure the BMCP subsystem.
   The installation process created a default started task called BMCP, which is located in the IPTSAMP library. Copy the BMCP started task into your SYSx proclib. Ensure that the IPTLIB library is APF-authorized before starting the subsystem.
   For information about operating the BMCP subsystem, see Operating subsystems and product servers (see page 258).
3. Run IPTCNTL(#ASMCOPT) to assemble and link the CPCOPT macro into the IPTLIB library.
4. Copy the newly-created members from IPTSAMP to your SYSx proclib. Based on your installation selections, four new members were created. Copy the cpcxUIM, cpcx, and cpcx IPT members to the SYSx proclib.
5. Customize the Log Analyzer ISPF interface.
   Log Analyzer includes a sample CLIST that you can use to invoke the Log Analyzer ISPF interface. This CLIST provides dynamic access to Log Analyzer libraries (through LIBDEF instructions) and displays the main menu of the Log Analyzer ISPF interface. You must configure the CLIST to point to the installed Log Analyzer libraries. You can also preset ISPF profile variables for the interface.
   a. Copy member LUICI@00 of the SAMP library to your system CLIST library.
   b. Edit member LUICI@00.
      - Change all instances of BMCNODE to the high-level qualifier <hlq> that was used to allocate the Log Analyzer libraries.
        The <hlq> is your user ID unless you changed the value of the PROFILE keyword in the job that expanded the installation image.
      - Change all instances of prd to the appropriate value based on whether you chose merged libraries or non-merged libraries during installation.
For more information about merged and non-merged libraries, see the product installation guide.

- If you chose merged libraries, change `prd` to `IM`.
- If you chose non-merged libraries, change `prd` to `LUI`.

Save the changes to member LUICI@00.

c. **(optional) Preset profile variables.**
   You can preset profile variables for all users of the interface. Edit member LUIZUSER of the PLIB library as explained in the comments.

d. Test the CLIST by entering the following command on any ISPF panel that accepts TSO commands:
   ```
   TSO %LUICI@00
   ```
   The Log Analyzer logo panel is displayed. When you press **Enter**, the Log Analyzer Main Menu is displayed.

6. When you complete the installation of the UIM server and CPC environments and copy the UIM- and CPC-related tasks to your SYSx proclib, you can start the product address spaces (i.e., MVS command `S cpcx`). This will automatically start your CPC-related product address space (i.e., `cpcxPT`).
   Once both address spaces have initialized, start the UIM server (for example, `S cpcxUIM`).
   For information about operating the UIM server, see Operating the UIM server (see page 234).

7. Install the console.
   For more information, see Customizing the console (see page 227).

---

**Customizing BMC System Communication for IMS**

This section describes customization tasks that are unique to BMC System Communication for IMS. Customizing refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered:

- Overview of customizing BMC System Communication for IMS (see page 17)
- BMC System Communication for IMS customization worksheet (see page 17)
- Completing BMC System Communication for IMS customization (see page 18)
Overview of customizing BMC System Communication for IMS

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and configuring the product libraries, see the Installation System documentation.

The customization tasks are unique to BMC System Communication for IMS.

Depending on the products that you are installing as part of this solution, you may also need to complete customization tasks that are applicable to the following BMC system administration products for IMS:

<table>
<thead>
<tr>
<th>Product</th>
<th>Location of configuration tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energizer for IMS Connect</td>
<td>Customizing Energizer for IMS Connect (see page 129)</td>
</tr>
<tr>
<td>Message Advisor for IMS</td>
<td>Customizing Message Advisor for IMS (see page 179)</td>
</tr>
</tbody>
</table>

BMC System Communication for IMS customization worksheet

Refer to the following worksheet as you work through the customization process for BMC System Communication for IMS.

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Customize the Log Analyzer ISPF interface.</td>
<td>Completing BMC System Communication for IMS customization (see page 18)</td>
</tr>
<tr>
<td></td>
<td>2. Start the UIM server.</td>
<td>Completing BMC System Communication for IMS customization (see page 18)</td>
</tr>
<tr>
<td></td>
<td>3. Install the console.</td>
<td>• Completing BMC System Communication for IMS customization (see page 18)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customizing the UIM server console (see page 228)</td>
</tr>
</tbody>
</table>
Completing BMC System Communication for IMS customization

This section describes the steps for customizing BMC System Communication for IMS.

1. Customize the Log Analyzer ISPF interface.
   Log Analyzer includes a sample CLIST that you can use to invoke the Log Analyzer ISPF interface. This CLIST provides dynamic access to Log Analyzer libraries (through LIBDEF instructions) and displays the main menu of the Log Analyzer ISPF interface. You must configure the CLIST to point to the installed Log Analyzer libraries. You can also preset ISPF profile variables for the interface.
   a. Copy member LUICI@00 of the SAMP library to your system CLIST library.
   b. Edit member LUICI@00.
      - Change all instances of BMCNODE to the high-level qualifier <hlq> that was used to allocate the Log Analyzer libraries.
        The <hlq> is your user ID unless you changed the value of the PROFILE keyword in the job that expanded the installation image.
      - Change all instances of prd to the appropriate value based on whether you chose merged libraries or non-merged libraries during installation.

   ![Note]

   For more information about merged and non-merged libraries, see the product installation guide.

   - If you chose merged libraries, change prd to IM.
   - If you chose non-merged libraries, change prd to LUI.

   Save the changes to member LUICI@00.
   c. (optional) Preset profile variables.
      You can preset profile variables for all users of the interface. Edit member LUIZUSER of the PLIB library as explained in the comments.
   d. Test the CLIST by entering the following command on any ISPF panel that accepts TSO commands:
      
      TSO %LUICI@00
      The Log Analyzer logo panel is displayed. When you press Enter, the Log Analyzer Main Menu is displayed.

2. Start the UIM server (for example, S uimServerName).
   For information about operating the UIM server, see Operating the UIM server (see page 234).
3. Install the console.
Customizing DELTA IMS and DELTA IMS VIRTUAL TERMINAL

This section describes customization tasks that are unique to the DELTA IMS and DELTA IMS VIRTUAL TERMINAL products. Customizing refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered:

- Overview of customizing DELTA IMS and DELTA IMS VIRTUAL TERMINAL (see page 19)
- DELTA IMS customization worksheet (see page 20)
- Updating IMS (see page 20)
- Updating MVS for APPC support (see page 23)
- Updating VTAM (see page 24)
- Adding DELTA IMS to TSO/ISPF (see page 26)
- Limiting access to DELTA IMS (see page 30)
- Setting global options (see page 37)
- Setting IMSID options (see page 42)
- Enabling the FDR feature (see page 49)
- Protecting DELTA Logs (see page 50)
- Modifying keyword tables (see page 50)
- Starting DELTA IMS (see page 51)

Overview of customizing DELTA IMS and DELTA IMS VIRTUAL TERMINAL

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and configuring the product libraries, see the Installation System documentation.

⚠️ Note

No configuration tasks were performed for the following BMC products for IMS:

- DELTA IMS
- DELTA IMS VIRTUAL TERMINAL
The configuration tasks that are described in this section apply to DELTA IMS and DELTA IMS VIRTUAL TERMINAL only.

DELTA IMS customization worksheet

Refer to the following worksheet as you work through the customization process for DELTA IMS:

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
</table>
| 1.   | Update IMS and VTAM. | Updating IMS (see page 20)  
|      |                   | Updating MVS for APPC support (see page 23)  
|      |                   | Updating VTAM (see page 24) |
| 2.   | Provide access to the ISPF interface through a CLIST or through an ISPF options menu. | Adding DELTA IMS to TSO/ISPF (see page 26)  
|      |                   | Accessing DELTA IMS from a CLIST (see page 26)  
|      |                   | Accessing DELTA IMS from an ISPF options menu (see page 27)  
|      |                   | Setting DELTA IMS default ISPF values (see page 28) |
| 3.   | Limit access to DELTA IMS through a SAF interface to RACF or through user access profiles. | Limiting access to DELTA IMS (see page 30)  
|      |                   | Implementing user access profiles (see page 31) |
| 4.   | Set global options. | Setting global options (see page 37) |
| 5.   | Set IMSID options for each control region that DELTA IMS services. | Setting IMSID options (see page 42) |
| 6.   | Enable the functionality of the FDR feature. | Enabling the FDR feature (see page 49) |
| 7.   | If the DELTA Logs are to be accessed from several CPUs, protect them from simultaneous update access. | Protecting DELTA Logs (see page 50) |
| 8.   | (optional) Modify keyword tables. | Modifying keyword tables (see page 50) |
| 9.   | Start DELTA IMS. | Starting DELTA IMS (see page 51) |

Updating IMS

This section describes the steps you must complete to update IMS.

1. Define spare elements.
   You can postpone this step until after the initial installation; however, you will have to perform another IMSGEN at a later time.
   For more information about defining spare elements, see the product user guide.
2. Add BMCLINK.
   Add the APPLCTN and TRANSACT macros that define BMCLINK to your IMS Stage-1 input as shown in the example below. You can replace the name BMCLINK with a name of your choice. If your site requires that IMS program names match PSB names, the BMCLINK program name is DLAXCTLO.

   **Warning**
   BMC does not recommend defining the BMCLINK program as a GPSB.

   ```
   APPLCTN  PSB=BMCLINK,PGMTYPE=(BATCH),
   SCHDTYP=SERIAL
   TRANSACT CODE=BMCLINK,AOI=YES
   ```

   **Note**
   - The transaction code is not required for DBCTL regions. The PSB and transaction names must match the names that are specified in member DLA#ACB of the DLACNTL library.
   - Type 1 AOI (CMD) command security Application programs can issue IMS commands by using the CMD communications call and retrieve the command response by using the GCMD communications call. These commands are called Type 1 AOI commands.

   A RESOURCE record with a resource name of $TRANCM1 controls the security for Type 1 AOI commands. To create an IMS RESOURCE record for Type 1 AOI commands, enter the following INSERT subcommand:

   ```
   INSERT DIVISION(musid|jobname) RESOURCE.qualifier -
   NAME($TRANCM1) TYPE(ICM|type) {VALIDATE|NOVALIDATE}
   ```

   The eTrust CA-ACF2 for IMS interface performs validation processing for Type 1 AOI (CMD) commands by default. If you do not want to secure Type 1 AOI commands, you must deactivate the eTrust CA-ACF2 for IMS interface validation processing for these commands. To deactivate this command validation, create an IMS RESOURCE record for Type 1 AOI commands that specifies NOVALIDATE.

   BMCLINK uses Type 1 AOI (CMD) processing.

   For additional information, see **eTrust CA-ACF2 for IMS documentation**.

3. If you will use DELTA IMS to customize one or more DBCTL regions, create BMCLINK subsystem control cards for the DBCTL regions. Otherwise, skip this step.
A member that contains a BMCLINK subsystem control card must be stored in the PROCLIB of each DBCTL region that will be customized through DELTA IMS. The member must take the form iiii ssss (where iiii is the IMSID of the DBCTL region and ssss is a four-character suffix that will be used for all BMCLINK subsystem control cards).

Note

BMC recommends that ssss be the same value that is specified for the SSM parameter in the DFSPBxxx member for this region.

If you have not already done so, specify a value for the SSM parameter in the DFSPBxxx member. You will use this value during this installation for DBCTL regions. This is the same value that you will specify in the IMSID IMS DBCTL region 'SSM' suffix name option later in the configuration process.

The PROCLIB member iiii ssss contains a control card. The control card format depends on the IMS version that you are running. For example, under IMS 14.1, the format is ssn, BMC1, DLABETB6.

The following table describes the information that you must provide in the control card.

**BMCLINK subsystem control card keywords for DBCTL regions**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssn</td>
<td>A one- to four-character BMCLINK subsystem name. It can be any name and it does not have to match any other name. This name is used in the /DIS SUBSYS ssn command.</td>
</tr>
<tr>
<td>BMC1</td>
<td>A literal value.</td>
</tr>
<tr>
<td>DLABETBx</td>
<td>The name of the external Subsystem Module Table, where x is one of the following suffixes for the corresponding IMS version: 4 for IMS Version 12.1, 5 for IMS Version 13.1, 6 for IMS Version 14.1</td>
</tr>
</tbody>
</table>

4. Perform an IMSGEN.

If you intend to use DELTA IMS to add resource elements (applications, databases, transactions, route codes), at least one of each type of resource element that is needed must be SYSGENed in the system. You should add at least one of the appropriate resource element(s) to the system at this time so that you do not have to perform another IMSGEN later.

5. Update AOIS.

Perform one of the following modifications, as appropriate, to the applicable type of IMS region:

- For DBCTL regions, update the AOIS keyword in PROCLIB member DFSPBxxx. You must specify a value that will authorize BMCLINK to issue IMS commands.
For IMS control regions, you must update IMS security. You can authorize BMCLINK to unlimited command use. However, you must at least authorize it to use the CHANGE command.

**Note**

If you used a transaction name other than **BMCLINK** in your IMS Stage-1 input, use the same name in the statements that you create to authorize IMS commands for BMCLINK.

6. Perform an IMS PSBGEN and ACBGEN.
A sample PSBGEN/ACBGEN job stream is provided in member DLA#ACB of the DLACNTL library (this is the job name only if you use the BMC defaults for the install JCL). The required PSB (with recommended IOASIZE) is as follows:

```
PSBGEN PSBNAME=BMCLINK,IOASIZE=1024,LANG=ASSEM
```

Use the following guidelines when you prepare for the PSBGEN:
- The PSB and transaction names (transaction name does not apply to DBCTL regions) must match the names that are specified in member DLA#ACB of the DLACNTL library.
- The IOASIZE value that you specify in your PSBGEN must match the value that you specify on the Global Options panel in the *Maximum DL/I command size* field. For more information, see Setting global options (see page 37).

**Updating MVS for APPC support**

Use the following procedure to update MVS for APPC support.

**Note**

This task is optional for DELTA IMS and does not apply to DELTA IMS for DBCTL.

To use DELTA IMS to modify APPC, you must update MVS with two modules that are provided by IBM.

**To update MVS for APPC support**

1. Add module ICQASLI0 to SYS1.PARMLIB(IKJTSO00).
The TSO/E module ICQASLI0 is located in data set SYS1.CMDLIB. Add this module name to the AUTHTSF name list in SYS1.PARMLIB(IKJTSO00).

2. Add the APPC/IMS TP_PROFILE scheduler exit to a LINKLIST data set. The IMSVS.RESLIB data set contains module DFSTPPE0, the APPC/IMS TP_PROFILE scheduler exit. Copy this module to a LINKLIST data set. Consult your MVS systems programmer to determine which LINKLIST data set to use.

Updating VTAM

This section describes the steps you must complete to update VTAM.

⚠️ **Note**

If you want to base your VTAM definition statements on BMC-provided sample statements, use the sample statements from member DLA$APPL of the DLASAMP library.

1. Assemble and link-edit the VTAM mode table. The VTAM mode table is supplied in member DLA#MODE of the DLACNTL library. You must assemble and link-edit the mode table into SYS1.VTAMLIB or its equivalent.

2. Create TSO/ISPF APPL definition statements in SYS1.VTAMLST for each TSO system that will run the DELTA IMS online interface.

Use the following guidelines when you create TSO/ISPF APPL definition statements:

- TSO LU names must be unique throughout your VTAM network.
- TSO ACBNAMEs must be unique only within a given MVS system.
- TSO ACBNAMEs must use the format `prefnnnn`, where `pref` is a four-character prefix used for all BMCLINK ACBNAMEs and `nnnn` is a number in a sequence that starts with 0001.
- BMC recommends that the TSO session identifier that begins each TSO/ISPF APPL definition match the corresponding TSO ACBNAME; however, a match is not required.

The following figure shows sample statements. Sample VTAM statements are also available in member DLA$APPL of the DLASAMP library.

**Sample TSO/ISPF APPL statements**

```plaintext
DLAU0001 APPL AUTH=(ACQ,PASS),MODETAB=DLAMODE, X
  DLOGMOD=DLAMOD1,EAS=1, X
  ACBNAME=DLAU0001

DLAU0002 APPL AUTH=(ACQ,PASS),MODETAB=DLAMODE, X
  DLOGMOD=DLAMOD1,EAS=1, X
  ACBNAME=DLAU0002

DLAU0003 APPL AUTH=(ACQ,PASS),MODETAB=DLAMODE, X
  DLOGMOD=DLAMOD1,EAS=1, X
```

BMC Software Confidential
Create one BMCLINK APPL statement for each BMCLINK started task that you will use.
BMCLINK LU names must be unique throughout your VTAM network.
The following figure shows a sample statement.

**Sample BMCLINK APPL statement**

```
BMCL0001 APPL AUTH=(ACQ,PASS),EAS=10
```

**Note**

One BMCLINK started task can be used to communicate with multiple IMS systems on the same CPU. You do not need to create a separate BMCLINK or APPL statement for each IMS system.

3. Create CDRSC statements if necessary.

<table>
<thead>
<tr>
<th>If the online interface and BMCLINK</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run on the same MVS system</td>
<td>Go to Step 4 (see page 25).</td>
</tr>
<tr>
<td>Do not run on the same MVS system in some or all cases</td>
<td>Use the following guidelines to create CDRSC statements.</td>
</tr>
</tbody>
</table>

Follow these guidelines when creating CDRSC statements:

- Each CDRSC LU name must match the LU name of the BMCLINK APPL statement that defines the BMCLINK task for the IMS system.
- The CDRM= parameter must identify the minor node where the BMCLINK task and IMS system will run.

The following figure shows sample statements.

**Sample CDRSC definition for MVST system**

```
VBUILD TYPE=CDRSC
DLAL0001 CDRSC CDRM=cdrmid
VBUILD TYPE=CDRSC
DLAL0002 CDRSC CDRM=cdrmid
```

4. Verify that the SYS1.VTAMLST member names, LU names, and ACBNAMEs that you created conform to your site’s standards and the requirements that are specified in this task.
5. If you have the required authority, activate the VTAM definition statements. Otherwise, verify that the definitions have been activated before proceeding with the configuration process.

Adding DELTA IMS to TSO/ISPF

This section describes the procedures for adding DELTA IMS to TSO/ISPF.

You can install the online interface so that you can invoke it from a CLIST or from an ISPF options menu. For more information, see Accessing DELTA IMS from a CLIST (see page 26) and Accessing DELTA IMS from an ISPF options menu (see page 27).

Accessing DELTA IMS from a CLIST

A sample CLIST that provides access to the online interface using LIBDEF is available in the SAMP library.

You can copy the SAMP library member into your CLIST library and update the applicable data set names to reference your data sets. The following table lists the DELTA IMS tiers, the SAMP library member that contains the sample CLIST, and the data set names that you need to update.

<table>
<thead>
<tr>
<th>DELTA IMS tier</th>
<th>Sample CLIST member</th>
<th>Data set names to update</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELTA IMS DLACI@00 &amp;DLALLIB</td>
<td>DLACI@00</td>
<td>&amp;DLALLIB</td>
</tr>
<tr>
<td>DELTA IMS DB/DC DLADBDC</td>
<td>DLADBDC</td>
<td>&amp;DLAMLIB</td>
</tr>
<tr>
<td>DELTA IMS for DBCTL DLADBCTL</td>
<td>DLADBCTL</td>
<td>&amp;DLAPLIB</td>
</tr>
<tr>
<td>DELTA IMS VIRTUAL TERMINAL DLAVT</td>
<td>DLAVT</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

The following DELTA IMS features do not support the LIBDEF service:

- DELTA IMS VIRTUAL TERMINAL TSS translate assist user exit
- DELTA IMS generate utility’s input user exit
- **TSOBMP (not available for DBCTL regions) to communicate with the IMS control region rather than BMCLINK**

If you attempt to use any of these functions under the LIBDEF environment, error messages will be issued. All other functions are fully supported under LIBDEF.
Accessing DELTA IMS from an ISPF options menu

Accessing DELTA IMS from an ISPF options menu requires that you pre-allocate the necessary ISPF data sets to the user.

You must add the following libraries to the TSO logon procedure for each user who requires access to DELTA IMS:

- Load library (ISPLLIB)
- ISPF panel library (ISPPLIB)
- ISPF message library (ISPMLIB)

⚠️ **Note**

- Consider the following points:
  - Load modules DLATSS, DLAXTSO0, DLAXALB0, and DLASAUT0 can be invoked internally as unauthorized TSO commands. If you use a facility to restrict access to TSO commands, you need to add the restricted TSO commands to the appropriate tables or rules so that DELTA IMS users can access them.
  - DELTA IMS supports the ISPF LIBDEF service for most functions. As a testing and migration aid, you can execute DLACI@00 in DLASAMP to dynamically invoke the ISPF interface without modifying your logon procedure.
  - There are additional tasks related to accessing DELTA IMS from an ISPF options menu. For more information, see Setting DELTA IMS default ISPF values (see page 28).

The following figure shows a sample ISPF/PDF Primary Option Menu that has been modified to access DELTA IMS.

**Sample modifications to ISPF/PDF Primary Option Menu**

```plaintext
%-----------------------  ISPF/PDF PRIMARY OPTION MENU  -----------------
%OPTION  ===>                                                           +
%   0 +ISPF PARMS  - Specify terminal and user parameters
%   1 +BROWSE      - Display source data or output listings
%   2 +EDIT        - Create or change source data
%   3 +UTILITIES   - Perform utility functions
%   4 +FOREGROUND  - Invoke language processors in foreground
%   5 +BATCH       - Submit job for language processing
%   6 +COMMAND     - Enter TSO command or CLIST
```
Setting DELTA IMS default ISPF values

After you install the TSO/ISPF panel and messages members for DELTA IMS, you may want to review and modify the default ISPF values for the variables that the product uses.

If any of these values are incorrect, DELTA IMS will prompt you for new values the first time that you invoke the online interface. You do not have to modify these values now; you can wait until an error is detected and correct it at that time. However, if several users are accessing the TSO/ISPF panels, each user must make the corrections when invoking the online interface.

DELTA IMS ISPF panel defaults
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;DLA4DATE</td>
<td>An eight-character, current date value. This value sets the last-modified or last-executed date within the product. As distributed, this date value uses the <code>mm/dd/yy</code> format; however, you can change the format to `yy/mm/dd, dd /mm/yy, and so on.</td>
</tr>
<tr>
<td>&amp;DLA4IMD</td>
<td>A four-character default IMSID value. As distributed, the default value is IMSA.</td>
</tr>
<tr>
<td>&amp;DLA4PDS</td>
<td>The name of the partitioned data set that will store DELTA Lists. You can specify up to 44 characters.</td>
</tr>
<tr>
<td>&amp;DLA4LIB</td>
<td>The product options load library data set name. This load library will store various product options and parameters that are used by the ISPF utilities and the BMCLINK region task. DLALIB is the recommended library name. You can specify up to 44 characters.</td>
</tr>
<tr>
<td>&amp;DLA4ALM</td>
<td>An option to specify whether an alarm should sound when ISPF messages are issued. Valid values are YES or NO.</td>
</tr>
<tr>
<td>&amp;DLA4BRV</td>
<td>An option to specify a work volume if the site does not support VIO- or SYSDA-type work file allocations. The default for most sites is a null value, &amp;Z.</td>
</tr>
<tr>
<td>&amp;DLA4BRU</td>
<td>An option to specify the generic unit name for temporary work file data sets. The default value for most sites is VIO.</td>
</tr>
</tbody>
</table>

The INIT section of ISPF panel DLAPl@00 contains several important default data set specifications.

You can override the date format, &DLA4DATE, and the data set names that are shown in the following figure.

**ISPF profile defaults for DELTA IMS**

```plaintext
/* ---------------------------------- /* USER-MODIFIABLE DEFAULTS */
&DLA4ALM = YES                      /* ISPF MSGS .ALARM=YES/NO */
&DLA4DATE = '&ZMONTH/&ZDAY/&ZYEAR'   /* DELTA IMS LAST-MOD DATE */
/                     */
IF (&DLA4IMD = &Z)               /* */
    &DLA4IMD = 'IMSA'            /* DEFAULT IMSID VALUE */
/                     */
&DLA4BRU = 'VIO'                  /* BROWSE WORK FILE UNIT */
&DLA4BRV = &Z                    /* BROWSE WORK FILE VOLSER */
/                     */
IF (&DLA4PDS = &Z)               /* */
    &DLA4PDS = 'BMCNODE.DELTAPDS' /* DELTA LIST PDS LIBRARY */
/                     */
IF (&DLA4LIB = &Z)               /* */
    &DLA4LIB = 'BMCNODE.DLA.LOAD' /* GLOBAL-PARMS LOADLIB */
/* -------------------------------------------------------------- */
```

For example, if you want to format dates as `yy/mm/dd`, modify the &DLA4DATE assignment statement as follows:

```plaintext
&DLA4DATE = '&2YEAR/&2MONTH/ZDAY' /*DELTA IMS LAST-MOD DATE*/
```
If your IMSID is PROD instead of the IBM-distributed default, you can modify the &DLA4IMD assignment as follows:

```
&DLA4IMD = 'PROD' /*DEFAULT IMSID VALUE*/
```

Within the limits of ISPF panel syntax, you can modify the above assignment statements to suit the environment at your site.

Once you have updated your logon procedure (proc), log off ISPF and log back on.

## Limiting access to DELTA IMS

By default, access to many DELTA IMS functions is unlimited.

To restrict product usage, you must take steps to protect the functions that you want to restrict.

Under most circumstances, you do not have to set security when initially installing DELTA IMS. Therefore, you may want to defer setting security until you have reviewed the various security methods.

DELTA IMS allows you to secure product features through either of the following methods:

- A System Authorization Facility (SAF) interface to RACF or an equivalent product
  
  For more information, see the *DELTA IMS User Guide*.

### Note

If you are going to restrict access to product functions via the SAF security interface, you must define the ACTIVATE resource before SAF will activate. The ACTIVATE resource provides a method to quickly activate and deactivate the interface. Users must have READ access to the ACTIVATE resource to access the product main menu. You should not define the ACTIVATE resource until you define all other resources.

### Warning

If your site is running ACF2 and you elect not to install the SAF security interface, you must add the following SAFDEF entry to your ACF2 parameters:

```
FUNCTION (4) FUNCRSN (0) ID (DELTA IMS) MODE (IGNORE)
RACROUTE (REQUEST=AUTH CLASS=DLA#) RETCODE (4)
```
Failure to add this SAFDEF entry may cause you to receive the following error message when attempting to perform any product function:

BMCDLANnnnnn NOT AUTHORIZED TO USE DELTA IMS

Adding this SAFDEF entry will ensure that your existing internal product security will be used. If you decide to use the SAF security interface at a later time, you must delete this SAFDEF entry from your ACF2 parameters.

- User access profiles
  For more information, see Implementing user access profiles (see page 31).

Implementing user access profiles

A user access profile is the user ID’s authorization for an IMSID.

All product functions that reference an IMS control region require specification of the control region’s IMSID. Before a user may designate an IMSID, a user access profile must exist for the userID and IMSID combination. The user access profile specifies that the user may access an IMSID during DELTA List processing. A user access profile also specifies the keyword table and suffix to be used for DELTA List Edit.

You can create new user access profiles, display existing user access profiles, and update user access profiles. For more information, see To create user access profiles (see page 31), To display existing user access profiles (see page 34), and To update user access profiles (see page 35).

To create user access profiles

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing DELTA IMS from an ISPF options menu (see page 27) or through the CLIST that you created in Accessing DELTA IMS from a CLIST (see page 26). The Primary Menu is displayed.
2. Type 5 in the selection field and press Enter. The Customization panel is displayed.
3. Type 3 in the selection field and press Enter. The Add User Access Profiles panel is displayed.

<table>
<thead>
<tr>
<th>UA</th>
<th>DELTA IMS DB/DC - Add User Access Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ===&gt;</td>
<td>__________________________________________________________</td>
</tr>
</tbody>
</table>

User profiles data set name: DLA.V5.DELTAUPF

Type a userid, an IMSID, the desired authorization values, and an optional keyword table suffix to define a user's authorization for an IMS system.

Type a userid, four asterisks '****', and the keyword table suffix to
define the default keyword table suffix for a given userid.

<table>
<thead>
<tr>
<th>Userid</th>
<th>IMSID</th>
<th>Exec/Check</th>
<th>IMS CMD</th>
<th>Parms</th>
<th>Display/Zap</th>
<th>A/S/N Cmds</th>
<th>Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

Authorization values
Type an 'A' for All, an 'S' for Some, or an 'N' for None to indicate whether the user may enter IMS commands. Type a 'Y' or 'N' to allow or disallow the other features.

Use the SAVE or END commands to permanently store all new profile entries; or Use the CANCEL command to discard any newly queued entries.

Note
If you use SAF security, you will only need to update the keyword table information in the UPF data set.

The following fields are available on this panel:

**User profiles data set name**
The name of the partitioned data set that contains all user access profiles. Each time you access this panel, this data set name defaults to the user profile data set name that is contained in DLA$GBL0. Changing the data set name on this panel does not update the data set name that is contained in DLA$GBL0.

**Userid**
Type a specific userID or a masking pattern.
When DELTA IMS performs an authorization check, it checks the most specific userIDs before the less specific userIDs until it finds a match. For example, assume user access profiles for IMSID IMSA existed for userIDs OPER1, OPER2, OPER*, and *. When DELTA IMS performed authorization checking for userID OPER3, it would select profile OPER* / IMSA. Profile OPER2 / IMSA would match userID OPER2, and * / IMSA would match userID TECH2 or any other userID.

**IMSID**
Type a specific IMSID or a masking pattern that can allow the user to access several IMSIDs.

**DELTA List Exec**
Type Y or N to indicate whether the user can execute a DELTA List.

**DELTA List Check**
Type Y or N to indicate whether the user can check a DELTA List.

**Execute IMS CM**
Type Y or N to indicate whether the user can issue IMS operator commands. This variable limits IMS commands that are issued from the Execute IMS Command panel only.
Note

Either Execute IMS Command authority or Update Parms authority is required to perform a TSS look-aside refresh.

Update Parms
Type Y or N to indicate whether the user can update the virtual terminal options. Update Parms authority is required to perform the following actions:

- Reload the product options in an active control region
- Perform log utility functions
- Refresh the CPU ID
- (DELTA IMS VIRTUAL TERMINAL only) refresh all TSS look-aside buffers in an active control region.

Storage Display
Type Y or N to indicate whether the user can display IMS control region storage.

Storage Zap
Type Y or N to indicate whether the user can apply zaps to IMS control region storage.

Warning

Enabling the Storage Display and Storage Zap options permits the product to display storage contents within the IMS address space at the TSO terminal. If misused, the Storage Display option can compromise data confidentiality. Users who can display IMS storage can also, if authorized, use the product to alter (or zap) storage. DELTA IMS and DELTA IMS VIRTUAL TERMINAL impose no restrictions over the MVS operating system or the data or addresses zapped. If misused, a loss of system integrity could result.

Allow A/S/N Cmds
Type A (All), S (Some), or N (None) to control the execution of IMS operator commands in DELTA Lists. A allows all IMS commands for the associated userID/IMSID combination, while N prohibits all IMS commands. S lets you individually allow or prohibit IMS commands.

Note

This field is ignored unless you specify to allow selected IMS operator commands on the Global Options panel. See Setting global options (see page 37).

keyword Table Suffix
If a customized keyword table has been created and should be implemented for the specified userID(s), type the keyword table name suffix that identifies the customized keyword table. Keyword tables specify defaults for DELTA List Edit sessions, DELTA Log reports, and DELTA IMS Check and Execute operations. For more information, see the *DELTA IMS User Guide*.

To display existing user access profiles

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in *Accessing DELTA IMS from an ISPF options menu* (see page 27) or through the CLIST that you created in *Accessing DELTA IMS from a CLIST* (see page 26). The Primary Menu is displayed.
2. Type 5 in the selection field and press Enter.
   The Customization panel is displayed.
3. Type 4 in the selection field and press Enter.
   The User Profile Sort panel is displayed.

### User Profile Sort panel

<table>
<thead>
<tr>
<th>UR</th>
<th>DELTA IMS DB/DC - User Profile Sort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ===&gt; __________________________________________________________</td>
<td></td>
</tr>
</tbody>
</table>

User profiles data set name: DLA.V5.DELTAUPF

Specify the collating sequence of the User Profiles and then press Enter to display the list of profiles.

- Sequence fields . . . . . . . . . . . . . . . 1 2 3  (major to minor - 1, 2, and 3)
- Ascending / Descending . . . . . . . A A A  (A or D)

<table>
<thead>
<tr>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>DELTA</th>
<th>Exec</th>
<th>Upd</th>
<th>IMS</th>
<th>Allow keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Modification</td>
<td>List</td>
<td>IMS</td>
<td>IMS</td>
<td>Storage</td>
<td>A/S/N</td>
<td>Table</td>
<td></td>
</tr>
<tr>
<td>Userid</td>
<td>IMSID Date</td>
<td>/ Time</td>
<td>Exc/Chk</td>
<td>CMDS</td>
<td>Parms</td>
<td>Dsply/Zap</td>
<td>cmds</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>-------</td>
<td>-----</td>
<td>------</td>
<td>------</td>
<td>-----</td>
<td>----</td>
</tr>
</tbody>
</table>

The following fields are available on this panel:

**User profiles data set name**
Type the name of the partitioned data set that contains all user access profiles.

**Sequence fields**
The sort sequence is from major to minor; 1 for first and 3 for last.

**Ascending/Descending**
Type the sort direction; A for ascending and D for descending.
To update user access profiles

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing DELTA IMS from an ISPF options menu (see page 27) or through the CLIST that you created in Accessing DELTA IMS from a CLIST (see page 26).

   The Primary Menu is displayed.

2. Type 5 in the selection field and press Enter.

   The Customization panel is displayed.

3. Type 4 in the selection field and press Enter.

   The User Profile Sort panel is displayed.

4. Specify the sequence of the fields and press Enter.

   The Update User Access Profiles panel is displayed.

### Update User Access Profiles Panel

<table>
<thead>
<tr>
<th>Act</th>
<th>Userid</th>
<th>IMSID</th>
<th>Date</th>
<th>Time</th>
<th>DELTA</th>
<th>Exec</th>
<th>Upd</th>
<th>IMS</th>
<th>IMS</th>
<th>Storage</th>
<th>A/S/N Table</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>AKG*</td>
<td>****</td>
<td>01/30/95 12:43:02</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARG</td>
<td>ARG2</td>
<td>01/04/95 15:58:02</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARG2</td>
<td>RCU3</td>
<td>01/18/95 10:41:49</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARG*</td>
<td>RCU*</td>
<td>01/18/95 10:42:04</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARG*</td>
<td>RCU*</td>
<td>01/18/95 10:42:27</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BSM</td>
<td>****</td>
<td>01/23/95 14:21:28</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BSM*</td>
<td>****</td>
<td>07/13/94 14:46:56</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>S</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CAC*</td>
<td>ISO*</td>
<td>11/08/94 13:49:19</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CAD2</td>
<td>CAD1</td>
<td>08/20/94 13:12:58</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

You can use the INSERT command to add a user access profile from the Update User Access Profiles panel.

Use the following format for the command, where `uuuuuuu` is a userID and `iii` is an IMSID:

```plaintext
INSERT userid imsid
```
6. **INSERT**

You can abbreviate the command to I. Generic characters are allowed.

The following fields are available on this panel:

**Act**

Type one of the following codes next to the appropriate userID:

- **S** Review or update the user's command authority.
- **D** Delete a profile.

**UserID**

A specific userID or a masking pattern.

**IMSID**

A specific IMSID or a masking pattern that can allow the user to access several IMSIDs.

**Last Modification Date/Time**

The date and time that the userID or IMSID was changed.

**DELTA List Exc/Chk**

Indicates whether the user can execute or check a DELTA List.

**Exec IMS CMDS**

Indicates whether the user can issue IMS operator commands. This variable limits IMS commands that are issued from the Execute IMS Command panel only.

**Upd IMS Parms**

Indicates whether the user can perform any of the following functions:

- Reload the product options in an active control region
- Perform log utility functions
- Refresh the CPU ID
- *(DELTA IMS only)* refresh all TSS look-aside buffers in an active control region

**IMS Storage Dsply/Zap**

Indicates whether the user can display or apply zaps to IMS control region storage.

**Warning**

If misused, the Storage Display option can compromise data confidentiality. Users who can display IMS storage can also, if authorized, use the product to alter (or zap) storage. DELTA IMS imposes no restrictions over the MVS operating system or the data or addresses zapped. If misused, a loss of system integrity could result.
Allow A/S/N cmds

A (All) indicates that all IMS commands for the associated userID/IMSID combination are allowed, N (None) indicates that all IMS commands are prohibited, and S (Some) indicates that specific IMS commands are allowed or prohibited.

Note

This field is ignored unless you specify to allow selected IMS operator commands on the Global Options panel. See Setting global options (see page 37).

keyword Table Suffix

The keyword table name suffix that identifies the customized keyword table, if a table has been created and implemented for the userID.

Setting global options

Use global options to specify parameters that govern DELTA IMS operations throughout your site, regardless of IMS system. You must review and save the global options if you are performing an initial installation of DELTA IMS.

DELTA IMS consists of various elements that are associated through VTAM and normal IMS inter-region communication. You must specify certain parameters to keep these elements operating according to the standards at your site. Global options apply to all TSO/ISPF sessions, batch functions, BMCLINK, and all control regions that DELTA IMS services. When you create or change global options, load module DLA$GBL0 is link-edited to your DELTA IMS options library.

Note

When global options are changed, other users must re-enter DELTA IMS to obtain the revised options. For proper operation, you should recycle BMCLINK.

To set global options

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing DELTA IMS from an ISPF options menu (see page 27) or through the CLIST that you created in Accessing DELTA IMS from a CLIST (see page 26).
   The Primary Menu is displayed.
2. Type 5 in the selection field and press Enter.
   The Customization panel is displayed.
3. Type 1 in the selection field and press Enter.
The Global Options (Page 1 of 2) panel is displayed.

<table>
<thead>
<tr>
<th>Command</th>
<th>DELTA IMS DB/DC - Global Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>GL</td>
<td>DELTA IMS DB/DC - Global Options</td>
</tr>
<tr>
<td>Scroll</td>
<td>PAGE</td>
</tr>
</tbody>
</table>

Global DELTA IMS options - Part I

Four character prefix for BMCLINK session ACBNAME . . BMCU

The WTO message routing codes . . . . . . . . . . . . . 11
The WTO message descriptor codes . . . . . . . . . . . 7

CHECK/EXECUTE pacing value (in 1/100s of seconds) . . 80
Request status check time interval (in seconds) . . . 20
Idle BMP automatic shutdown interval (in seconds) . . 300

Maximum DL/I command size (in bytes) . . . . . . . . 1024
(Size must match PSBGEN IOASIZE specified for the BMCLINK PSB.
Press HELP for more information.)

BMCLINK ENQ qname . . . . . . . . . . . . . . . . . . . BMCLINK
BMCLINK ENQ rname (VTAM interface) . . . . . . . . . BMCLINKV
BMCLINK ENQ rname (BMP control) . . . . . . . . . . . BMCLINKB
IMSID options update ENQ qname . . . . . . . . . . . . DLAIMSID

Use the SAVE command to save options.

The following fields are available on this panel:

**Four character prefix for BMCLINK session ACBNAME**
Specify the four-character prefix of the VTAM ACB name that is used for the TSO half of the VTAM LU-LU session with BMCLINK. The actual ACB name that is used will be the first available beginning with pppp 0001, pppp 0002, etc.

A user session is established anytime a user enters DELTA IMS. When necessary, a VTAM LU-LU connection is made between the DELTA IMS session and a BMCLINK task. This connection is known as a BMCLINK user session. The actual BMCLINK task that is contacted depends on the VTAM LU-name that is specified in the IMSID basic options for the specified IMS control region.

**The WTO message routing codes**
Specify one or more of the WTO routing codes, separated by commas, to be used by DELTA IMS and BMCLINK. BMCLINK issues WTO messages any time significant events occur. Use the WTO routing code to direct these messages to selected consoles.

**The WTO message descriptor codes**
Specify one or more of the WTO message descriptor codes, separated by commas, to be used by DELTA IMS and BMCLINK. BMCLINK issues WTO messages any time significant events occur. You can suppress these messages depending on the WTO message descriptor code specified.

**CHECK/EXECUTE pacing value (in 1/100s of seconds)**
Specify a pacing value in hundredths of a second to control the wait time between the execution of successive lines in a DELTA List. For example, if you specify a pacing value of 50, the Check and Execute functions check or execute the individual lines of a DELTA List at half-second intervals.

**Request status check time interval (in seconds)**
Specify the frequency between status messages, in seconds. BMCLINK periodically responds to the BMCLINK user session while processing a request for that session so that the user stays informed of the request processing status.

**Idle BMP automatic shutdown interval (in seconds)**
Specify the period of time, in seconds, after which BMCLINK should consider a BMP inactive and terminate it. BMCLINK communicates with an IMS control region by creating an IMS BMP task for that IMSID.

**Maximum DL/I command size (in bytes)**
Specify the size of the largest DL/I command to be issued through DELTA IMS. Commands and responses are shipped between BMCLINK and IMS when you execute and check DELTA Lists or process IMS commands. The value specified is the size of the area that is used to hold these commands and responses. The value must be the same as the value that is specified in the PSB IOASIZE field for the BMCLINK program (IMS and DBCTL control regions) and the BMCLINK transaction (IMS control regions only).
The default is 1024 bytes, which is the recommended size. If you specify a value that is less than 1024 bytes, you cannot use the same BMCLINK to support communication for both DELTA IMS and ETA.

**BMCLINK ENQ qname**
BMCLINK uses ENQ/DEQ to serialize certain internal activities. The scope of the ENQ extends only to its address space, not to the entire system. If necessary, you can specify the ENQ qname and rnames to conform to the standards at your site.

**BMCLINK ENQ rname (VTAM interface)**
Specify the ENQ rname for the VTAM interface.

**BMCLINK ENQ rname (BMP control)**
Specify the ENQ rname for BMP control.

**IMSID options update ENQ qname**
DELTA IMS uses ENQ/DEQ to serialize the creation and modification of options that are associated with a given IMSID. Specify the systems level qname to be used to prevent concurrent access and overwrite of a given set of IMSID basic options.

4. After you specify the information on the Global Options (Page 1 of 2) panel, press Enter. The Global Options (Page 2 of 2) panel is displayed.
Generic DASD unit name . . . . . . . . . . . . . SYSDA__

User profiles data set name DLA.V5.DELTAUPF______________________________

DELTA List options. Select one from each group. Then press Enter.

Userid for authorization check . . 1 1. Active userid
  2. Last-update userid

History information . . . . . . . . 1. None
  2. Record each time executed

IMS operator commands . . . . . 2 1. Allow all commands
  2. Allow selected commands
  3. None allowed

Use the SAVE command to save options.

The following fields are available on this panel:

**Internal trace table size (in 1k multiples)**
Specify the internal trace table size, in 1024-byte increments. The Internal Trace facility is always active within BMCLINK. It maintains a log of all significant events in a virtual storage table, which is primarily intended for BMC diagnostic purposes. The trace table minimum recommended size is 16K.

**Internal trace table dynamic dump sysout class**
Specify the sysout class to be used if the internal trace table appears in any abend dumps. This class is also used if you must print the table on demand.

**Generic DASD unit name**
Specify the generic DASD unit name that the DELTA Log List function uses to allocate work files and temporary report files during sorts.

**User profiles data set name**
Specify the name of the data set where the user access profiles reside. This name is assigned at installation.

**Userid for authorization check**
Select one of the following options to indicate which user ID is presented to the User Authorization routine exit and recorded in the DELTA Log when a DELTA List Check or Execute is initiated:

- 1 Active userid
- 2 Last-update userid

**IMS operator commands**
Select one of the following options to allow all, some, or no IMS operator commands. For a graphic representation of these options, see Figure 3 (see page 41).

- 1 Allow all commands
- 2 Allow selected commands: Option 2 causes DELTA IMS to examine the user access profile and determine which IMS operator commands in the DELTA List are allowed.
- 3 None allowed
Note

If user profiles are used to control access to IMSID-related functions, this value controls the ability to enter IMS commands from within DELTA Lists. If the SAF security interface is used, this value is ignored.

The following figure shows the security hierarchy for commands in a DELTA List.

Security hierarchy for commands in a DELTA List

5. Press **F3** to save changes to the global options.
Setting IMSID options

This section describes the procedures for setting IMSID options.

You should set IMSID options if you are performing an initial installation of DELTA IMS.

For DELTA IMS to access an IMS system, you must define the system to DELTA IMS with a set of IMSID options. When you create or change IMSID options, load module DLA#*** (where *** is the IMSID) is link-edited to your DELTA IMS options library.

You must create IMSID basic options for each control region that DELTA IMS services.

To specify site-defined default values that will prime new IMSID basic options modules, you can create and save a set of options for an IMSID named DFLT. This action will create an options module named DLA#DFLT that will prime the IMSID basic options when you define new systems. For more information, see To create a new IMSID (see page 42).

Once you have saved the IMSID options module, the changes will only take place during the next IMS restart unless you perform an IMSID options REFRESH.

Note

For a number of reasons, exercise extreme care when refreshing the IMSID basic options. Consider the following:

- Certain parameter changes will not take effect until the next IMS restart. These parameters are marked with an asterisk (*) on the DELTA IMS configuration panels.
- Each reload of the IMSID basic options will permanently use, on an accumulating basis, approximately 1024 bytes of IMS private storage. If this amount of storage becomes significant or if you do not have a complete understanding of the impact of this kind of change, postpone updates to the IMSID options until the next IMS restart.

To create a new IMSID

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing DELTA IMS from an ISPF options menu (see page 27) or through the CLIST that you created in Accessing DELTA IMS from a CLIST (see page 26).

The Primary Menu is displayed.

2. Type 5 in the selection field and press Enter.
The Customization panel is displayed.

3. Determine the method that you want to use to create the new IMSID:

<table>
<thead>
<tr>
<th>To create the new IMSID by</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using DELTA IMS defaults</td>
<td>Step 4 (see page 43)</td>
</tr>
<tr>
<td>Copying options from an existing IMSID</td>
<td>Step 5 (see page 43)</td>
</tr>
</tbody>
</table>

⚠️ **Note**

If you are creating a new IMSID module, DELTA IMS is disabled by default.

4. Type the name of the new IMSID in the **for IMSID** field and press **Enter**.
   The IMSID basic options will be copied from the defaults in DLA#DFLT, if it exists.
   You can specify the defaults that will be used when you create a new set of IMSID basic options. To specify the IMSID basic options default values, create a set of options for IMSID DFLT as if it were a valid IMSID. This action creates load module DLA#DFLT, which primes the IMSID Options fields whenever you define a new IMSID.

5. Type the name of the existing IMSID in the **for IMSID** field and press **Enter**.
   The IMSID Options panel is displayed.

**IMSID Options panel**

6. Type over the new IMSID and press **Enter**.
   The new options will be copied from the existing IMSID.
For DELTA IMS to be active for the next IMS restart, it requires a copy of the IMSID basic options module to be present in the IMS control region STEPLIB data set. You can copy the IMSID basic options module to the appropriate library or allow DELTA IMS to link-edit a copy to the STEPLIB data set. When DELTA IMS performs this copy for you, the overridden IMSID is used in the options module name instead of the unique IMSID; and it is copied to any libraries that you specified in the When saved, IMSID options will be copied to these additional libraries fields on the IMSID Options panel.

To set IMSID options

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing DELTA IMS from an ISPF options menu (see page 27) or through the CLIST that you created in Accessing DELTA IMS from a CLIST (see page 26). The Primary Menu is displayed.
2. Type 5 in the selection field and press Enter.
   The Customization panel is displayed.
   a. Type 2 in the selection field and press Enter.
   The IMSID Options panel (see page 42) is displayed. The following fields are available on this panel:

   **IMSID**
   Specify the IMSID of the IMS control region for which you want to set IMSID options. The IMSID must be unique for those IMS systems that DELTA IMS will access through BMCLINK.
   Select one of the following choices allow you to modify options for a control region that DELTA IMS services. If you have previously installed DELTA IMS and want to change options that you previously specified, select one of the following options and press Enter. If you are performing an initial installation, skip this field, complete the next field, and see To create a new IMSID (see page 42) for instructions on creating a new IMSID.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSID basic options</td>
<td>For more information, see To set IMSID basic options (see page 45).</td>
</tr>
<tr>
<td>BMCLINK and DELTA Log options</td>
<td>For more information, see To set BMCLINK, Delta Log, and APPC options (see page 48).</td>
</tr>
<tr>
<td>Options 3 through 8</td>
<td>These options apply only to DELTA IMS. For more information, see the DELTA IMS VIRTUAL TERMINAL User Guide.</td>
</tr>
<tr>
<td></td>
<td>• 3 Limits for Virtual Terminal</td>
</tr>
<tr>
<td></td>
<td>• 4 Options for Virtual Terminal</td>
</tr>
<tr>
<td></td>
<td>• 5 TSS tables for Virtual Terminal</td>
</tr>
<tr>
<td></td>
<td>• 6 Logon for Virtual Terminal</td>
</tr>
<tr>
<td></td>
<td>• 7 Signon Bypass for Virtual Terminal</td>
</tr>
<tr>
<td></td>
<td>• 8 Signon for Virtual Terminal</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>U Update options in the IMS control region</strong></td>
<td>This option applies to all of the DELTA IMS tiers. Specify this option to send a request to the online IMS system to reload the IMSID options from the standard IMS control region STEPLIB/JOBLIB/link-list concatenation. Depending on the options you select, a confirmation panel may be displayed before the control region is updated. If the IMSID options module that the control region loads matches the options module that the IMSID Options panel saves, message <strong>BMC2005 'IMS OPTIONS UPDATED'</strong> is returned. The IMSID options module is reloaded in the active control region indicated by the options. If the options module that the control region loads does not match the module saved, message <strong>BMC2030 'OPTIONS NOT UPDATED'</strong> is returned. This message indicates that the module loaded from the control region STEPLIB/JOBLIB/link-list does not match the one saved by the ISPF interface. Verify that the library name that is specified in the IMS control or DBCTL region STEPLIB matches the library name that is specified in the IMSID options.</td>
</tr>
<tr>
<td><strong>R Refresh CPU-ID in the IMS control region</strong></td>
<td>This option applies to all of the DELTA IMS tiers. Specify this option to send a request to the online IMS system to refresh the CPU ID security from the standard STEPLIB/JOBLIB/link-list concatenation of your control region JCL. The update is applied without a restart of your IMS control region. Depending on the options you select, a confirmation panel may be displayed before the CPU ID is refreshed. This process only pertains to changing your options while IMS is up. If IMS is not up, the refresh process is not needed since changes are picked up after the next restart.</td>
</tr>
<tr>
<td><strong>When saved, IMSID options will be copied to these additional libraries</strong></td>
<td>If you want to store additional copies of your IMSID options, use this field to specify the names of the libraries to use. No additional copies of the IMSID options will be made if you leave these fields blank.</td>
</tr>
</tbody>
</table>

**To set IMSID basic options**

1. Type **1** in the selection field of the IMSID Options panel and press **Enter**.
   The IMSID Basic Options (Page 1 of 8) panel is displayed.
The following fields are available on this panel:

**IMSID**
If you overtype the IMSID with the name of an existing IMSID, any changes to the original options are saved and the new IMSID options are loaded for update. If the new IMSID does not exist, the new set of options are copied from the previous IMSID options.

**Override IMSID**
If you do not have unique IMSIDs, specify the non-unique IMSID in this field. The override IMSID is used in the parameters that are passed to the IMS region controller in the BMCLINK BMP subtask. It is also stored in the log control record of each DELTA Log data set. The IMSID options module, DLA# (where # is the IMSID) in an IMS control region STEPLIB library, uses the override IMSID rather than the unique IMSID. This field is automatically primed with the unique IMSID. Blanks are not acceptable.

**IMS version/release level (121,131,141)**
Specify the IMS version for this IMSID: 121 for IMS Version 12.1, 131 for IMS Version 13.1, 141 for IMS Version 14.1. An IMS level is specified for each IMSID that DELTA IMS services; therefore, DELTA IMS can support a mixture of IMS systems.

**DELTA IMS system log code (A0-FF)**
Type the log code that DELTA IMS will use when it writes records to the IMS system log. Use any hexadecimal number from X'A0' to X'FF'. The default is X'DE'. You must cold-start IMS to change this value.

**User authorization exit name**
Specify the name of a user-written exit routine. This exit is invoked in the BMP address space for each transaction that is transmitted to IMS. This exit routine may inspect, alter, or reject the transaction.

**User customization exit name**
Specify the name of a user-written exit routine. This exit is invoked in the user address space for each transaction that is transmitted to IMS. This exit routine may inspect, alter, or reject the transaction.
1. **Note**

The Options library which contains this exit routine must be allocated to the user’s TSO session (TSO ALLOC command or in the TSO user’s TSO PROC ISPLLIB file allocation). Otherwise, the following error message will occur:

```
BMC1663 USER EXIT ######## NOT FOUND
```
4. Complete the following fields only for DBCTL systems:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is this a DBCTL region? (YES, NO)</td>
<td>If this is a DBCTL region, type YES and complete the following fields. Otherwise, type NO and ignore the following fields.</td>
</tr>
<tr>
<td>IMS DBCTL region &quot;SSM=&quot; suffix name</td>
<td>SSM is the same value that is specified for the SSM parameter in the DFSPBxxx member for this region. Type the suffix in this field.</td>
</tr>
<tr>
<td>IMS PROCLIB data set</td>
<td>Specify the name of the PROCLIB data set that contains the member that stores IMS subsystem parameters, including those that are used for the BMCLINK subsystem.</td>
</tr>
</tbody>
</table>

To set BMCLINK, Delta Log, and APPC options

Type 2 in the selection field of the IMSID Options panel or press DOWN on the IMSID Basic Options (Page 1 of 8) panel and press Enter.

The IMSID Basic Options (Page 2 of 8) panel is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSID</td>
<td>If you overtype the IMSID with the name of an existing IMSID, any changes to the original options are saved and the new IMSID options are loaded for update. If the new IMSID does not exist, the new set of options is copied from the previous IMSID options.</td>
</tr>
<tr>
<td>BMCLINK TRANSACTION CODE and BMCLINK PSB name</td>
<td>For DBCTL control regions, specify a BMCLINK PSB name only. For IMS control regions, specify the transaction code and PSB name that BMCLINK will use to attach the IMS region controller.</td>
</tr>
<tr>
<td>BMCLINK task network LU-name</td>
<td></td>
</tr>
</tbody>
</table>
Specify a network LU-name for the BMCLINK task portion of the BMCLINK user session that will be established with one or more users. For non-DBCTL IMS systems, you can type **TSOBMP to create a non-VTAM BMCLINK. The TSO user must be logged on to the MVS system on which the particular IMS is running.

**IMS RESLIB data set name**

Specify the RESLIB data set name. The IMS RESLIB name is required to determine where DELTA IMS can find IMS BMP service routines in modules DFSRRC00 and DFSRRC40. These modules are typically stored in the IMS RESLIB data set.

**Primary log and Secondary log**

Specify the primary and secondary DELTA Log data set names. Once DELTA IMS has been activated for the IMS control region, these data sets must be available during IMS initialization; otherwise, restart fails. For more information about DELTA Logs, see the DELTA IMS User Guide.

**Format the logs**

Type / to allocate and format the log data sets. The Log Allocate/Format panel prompts you for log allocation attributes. You can also access this panel from the Primary Menu under option 6 (Utilities). For more information about log reports, see the DELTA IMS User Guide.

**Warning**

By reformatting, you can destroy the DELTA Log data sets that are currently established. These data sets contain updates to an IMS control region and should not be formatted unless you intend to remove all DELTA IMS updates and then cold-start IMS.

**APPC/MVS data set names**

Note

This option does not apply to DELTA IMS for DBCTL.

If you plan to use DELTA IMS to update APPC, specify the name of the TP_PROFILE data set that you will use.

---

**Enabling the FDR feature**

You must complete the following steps to enable the functionality of the FDR feature.

1. Add the DELTA IMS library to the STEPLIB for the FDR region.
2. Ensure that the ACBLIB in the FDR region is the same as in the control region.
3. Verify that DELTA IMS is licensed on the CPU where the FDR region resides.
4. Specify the IMSID of the FDR region in the XRF/FDR alternate IMSID field when you are setting the IMSID basic options for the primary IMSID options module.
5. When you save your IMSID options, DELTA IMS automatically creates two IMSID options modules. The primary IMSID options module is named DLA#iii (where iii is the IMSID of your primary system). The second IMSID options module is named DLA#fff (where fff is the IMSID of the system where the FDR region resides). DELTA IMS creates these modules automatically to ensure that they are always synchronized.

**Note**
MODBLKS DD is not needed in FDR JCL

Warning

Never manually edit the IMSID options module for your FDR region. To avoid potential errors, the options for the primary IMSID options module and the FDR region IMSID options module must not conflict.

Protecting DELTA Logs

If the DELTA Logs are to be accessed from several CPUs, you must protect them from simultaneous update access.

The products issue a systems-level enqueue with an 8-byte QNAME of DELTAIMS and a 44-byte RNAME that is equivalent to the data set name of the DELTA Logs. This enqueue should be in effect for short periods while the DELTA Logs are being read or written. The enqueue combination should be defined to the MVS product (such as GRS or its equivalent) that provides cross-system protection at your site.

Modifying keyword tables

You can modify the keyword tables for the following purposes:

- Tailor default values that are used in DELTA List Edit to your site’s standards
- Refine DELTA List-related displays and reports
- Restrict the set of supported parameters and values that are used by individual DELTA IMS users and/or groups of DELTA IMS users

Note

This task does not apply to DELTA IMS.

For more information about creating DELTA IMS keyword tables, see the administrative section in the DELTA IMS User Guide.
Starting DELTA IMS

You must start DELTA IMS after you complete the other configuration tasks that are described in this section.

1. Update the IMS control or DBCTL region and DLI SAS, if applicable, to include the APF-authorized library in the STEPLIB concatenation. The APF-authorized library must precede the IMS RESLIB in the STEPLIB concatenation.

   **Note**

   BMC recommends that you execute the IMS system from a STEPLIB or JOBLIB. If it is unacceptable at your site to execute IMS from a STEPLIB or JOBLIB, you must use ddname BMCRESLB to allocate the IMS RESLIB that is accessed from the LINKLIST to IMS.

2. Start BMCLINK.

   BMCLINK allows users to communicate with an IMS system. TSO-based users of IMS and DELTA IMS do not have to run on the same CPU. Start the BMCLINK job (or started task) on each CPU where an IMS system that is serviced by DELTA IMS will run. DLACNTL member DLA#LINK provides sample JCL for BMCLINK.

   **Note**

   BMC recommends that you stop BMCLINK before shutting down IMS. If you attempt to execute a DELTA List after issuing a `/CHKPT FREEZE` or `DUMPQ`, a user abend 168 will occur if the DELTA Log is not updated in time. Stopping BMCLINK before shutting down IMS will prevent any last-minute execution of DELTA IMS.

3. Process the CPU ID password (either bypass or permanent) that will allow DELTA IMS to work.

   For more information, see the Installation System documentation.

   **Note**

   A separate password is required for DELTA IMS for DBCTL.

4. Cold start IMS.
Customizing DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL

This section describes configuration tasks that are unique to the DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL products. Customizing refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered:

- Overview of customizing DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 52)
- DELTA PLUS customization worksheet (see page 53)
- Updating IMS1 (see page 54)
- Updating VTAM In DLA and DLP (see page 54)
- Adding the products to TSO/ISPF (see page 56)
- Limiting access to the products (see page 59)
- Setting global options in DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 71)
- Setting IMSID options when installing DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL (see page 75)
- Enabling the FDR feature (DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL) (see page 82)
- Setting Group options (see page 83)
- Refreshing CPUID options (see page 87)
- Creating and formatting Log and History File data sets (see page 88)
- Creating View Profiles (see page 90)
- Editing View Profiles (see page 96)
- Allocating new data sets (see page 104)
- Adding an IMSID to an existing Group’s Log data sets (see page 107)
- Completing DELTA PLUS VIRTUAL TERMINAL customization (see page 109)
- Starting products (see page 127)
- DELTA PLUS VIRTUAL TERMINAL customization worksheet (see page 127)

Overview of customizing DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL

You should complete the customization tasks after you have installed and customized the product libraries through the Installation System.

For information about installing and customizing the product libraries, see the Installation System documentation.
Note

No configuration tasks were performed for the following BMC products for IMS:

- DELTA PLUS
- DELTA PLUS VIRTUAL TERMINAL

The customization tasks that are described in this section apply to DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL only.

DELTA PLUS customization worksheet

Refer to the following worksheet as you work through the customization process for DELTA PLUS.

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Update IMS and VTAM.</td>
<td>- Updating IMS1 (see page 54)&lt;br&gt;- Updating VTAM in DLA and DLP (see page 54)</td>
</tr>
<tr>
<td></td>
<td>2. Provide access to the ISPF interface through a CLIST or through an ISPF options menu.</td>
<td>- Adding the products to TSO/ISPF (see page 56)&lt;br&gt;- Accessing the products from a CLIST (see page 57)&lt;br&gt;- Accessing the products from an ISPF options menu (see page 57)</td>
</tr>
<tr>
<td></td>
<td>3. Limit access to DELTA PLUS through user access profiles, a SAF interface to RACF, or TopSecret.</td>
<td>- Limiting access to the products (see page 59)&lt;br&gt;- Implementing user access profiles and UPF security (see page 60)&lt;br&gt;- Implementing a SAF interface to RACF (or equivalent) product (see page 67)&lt;br&gt;- Implementing TopSecret (see page 70)</td>
</tr>
<tr>
<td></td>
<td>4. Set global options.</td>
<td>Setting global options in DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 71)</td>
</tr>
<tr>
<td></td>
<td>5. Set IMSID options for each control region that DELTA PLUS services.</td>
<td>Setting IMSID options when installing DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL (see page 75)</td>
</tr>
<tr>
<td></td>
<td>6. Enable the functionality of the FDR feature.</td>
<td>Enabling the FDR feature (DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL) (see page 82)</td>
</tr>
<tr>
<td></td>
<td>7. (optional) Set Group options.</td>
<td>Setting Group options (see page 83)</td>
</tr>
<tr>
<td></td>
<td>8. Refresh the CPUID options.</td>
<td>Refreshing CPUID options (see page 87)</td>
</tr>
<tr>
<td></td>
<td>9. Create and format the Log and History File data sets.</td>
<td>Creating and formatting Log and History File data sets (see page 88)</td>
</tr>
<tr>
<td></td>
<td>10. If this is the first time you are installing DELTA PLUS at your site, create View Profiles.</td>
<td>Creating View Profiles (see page 90)</td>
</tr>
</tbody>
</table>
Updating IMS1

This section describes the steps you must complete to update IMS.

1. Define spare elements.
   You can postpone this step until after the initial installation; however, you will have to perform another IMSGEN at a later time.
   For more information about defining spare elements, see the product user guide.

2. Perform an IMSGEN.
   If you intend to use the product to add resource elements (applications, databases, transactions, route codes), at least one of each type of resource element that is needed must be SYSGENed in the system. You should add at least one of the appropriate resource element(s) to the system at this time so that you do not have to perform another IMSGEN later.

Updating VTAM In DLA and DLP

This section describes the steps you must complete to update VTAM.

⚠️ Note

If you want to base your VTAM definition statements on BMC-provided sample statements, use the sample statements from member DLP$APPL of the DLPSAMP library.

1. Assemble and link-edit the VTAM mode table.
   The VTAM mode table is supplied in member DLP$MODE of the DLPCNTL library. You must assemble and link-edit the mode table into SYS1.VTAMLIB or its equivalent.

⚠️ Warning
1. If you are a DELTA IMS user and you are installing DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL, you cannot use the BMCLINK VTAM mode table. If you do, BMCXLINK will issue the following message:

```
BMCDLP18770E VTAM OPEN RC=X'***', FDBK2=X'***', incorrect
RUSIZES from MODETAB
```

2. Create TSO/ISPF APPL definition statements in SYS1.VTAMLST for each TSO system that will run the product online interface.

Use the following guidelines when you create TSO/ISPF APPL definition statements:

- TSO LU names must be unique throughout your VTAM network.
- TSO ACBNAMEs must be unique only within a given MVS system.
- TSO ACBNAMEs must use the format `prefnnnn`, where `pref` is a four-character prefix used for all BMCXLINK ACBNAMEs and `nnnn` is a number in a sequence that starts with 0001.
- BMC recommends that the TSO session identifier that begins each TSO/ISPF APPL definition statement match the corresponding TSO ACBNAME; however, a match is not required.

The following figure shows sample statements. Sample VTAM statements are also available in member DLP$APPL of the DLPSAMP library.

**Sample TSO/ISPF APPL statements**

```
DLP0001  APPL  AUTH=(ACQ,PASS),MODETAB=DLPMODE, X
          DLOGMOD=DLPMOD1,EAS=1, X
          ACBNAME=DLP0001
DLP0002  APPL  AUTH=(ACQ,PASS),MODETAB=DLPMODE, X
          DLOGMOD=DLPMOD1,EAS=1, X
          ACBNAME=DLP0002
DLP0003  APPL  AUTH=(ACQ,PASS),MODETAB=DLPMODE, X
          DLOGMOD=DLPMOD1,EAS=1, X
          ACBNAME=DLP0003
DLP0004  APPL  AUTH=(ACQ,PASS),MODETAB=DLPMODE, X
          DLOGMOD=DLPMOD1,EAS=1, X
          ACBNAME=DLP0004
DLP0005  APPL  AUTH=(ACQ,PASS),MODETAB=DLPMODE, X
          DLOGMOD=DLPMOD1,EAS=1, X
          ACBNAME=DLP0005
```

Create one BMCXLINK APPL statement for each BMCXLINK started task that you will use. BMCXLINK LU NAMES must be unique throughout your VTAM network. The following figure shows a sample statement.

**Sample BMCXLINK APPL statement**

```
DLPX0001 APPL AUTH=(ACQ,PASS), EAS=10
```
Note

One BMCXLINK can be used to service all IMS systems in the entire XCF complex. The only restriction is that if you are using Groups, a single BMCXLINK must be used for all requests against a Group.

3. Create CDRSC statements if necessary.

<table>
<thead>
<tr>
<th>If the online interface and BMCXLINK</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run on the same MVS system</td>
<td>Go to Step 4 (see page 56).</td>
</tr>
<tr>
<td>Do not run on the same MVS system in some or all cases</td>
<td>Use the following guidelines to create CDRSC statements.</td>
</tr>
</tbody>
</table>

Follow these guidelines when creating CDRSC statements:

- Each CDRSC LU name must match the LU name of the BMCXLINK APPL statement that defines the BMCXLINK task for the IMS system.
- The CDRM= parameter must identify the minor node where the BMCXLINK task and IMS system will run.

The following figure shows sample statements.

**Sample CDRSC definition for MVST system**

```
VBUILD TYPE=CDRSC
DLPL0001 CDRSC CDRM=cdrmid
VBUILD TYPE=CDRSC
   DLPL0002 CDRSC CDRM=cdrmid
```

4. Verify that the SYS1.VTAMLST member names, LU names, and ACBNAMEs that you created conform to your site’s standards and the requirements that are specified in this task.

5. If you have the required authority, activate the VTAM definition statements. Otherwise, verify that the definitions have been activated before proceeding with the configuration process.

## Adding the products to TSO/ISPF

This section describes the procedures for adding DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL to TSO/ISPF.

You can install the online interface so that you can invoke it from a CLIST or from an ISPF options menu. For more information, see Accessing the products from a CLIST (see page 57) and Accessing the products from an ISPF options menu (see page 57).
Accessing the products from a CLIST

For each product, a sample CLIST that provides access to the online interface using LIBDEF is available in the SAMP library.

You can copy the SAMP library member into your CLIST library and update the applicable data set names to reference your data sets. The following table lists the products, the SAMP library member that contains the sample CLIST, and the data set names that you need to update.

**Sample CLIST members and associated data sets for CLIST access to products**

<table>
<thead>
<tr>
<th>Product</th>
<th>Sample CLIST member</th>
<th>Data set names to update</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELTA PLUS</td>
<td>DLPCI@00</td>
<td>&amp;DLPLLIB</td>
</tr>
<tr>
<td>DELTA PLUS for DBCTL</td>
<td>DTDCI@00</td>
<td>&amp;DLPLIB &amp;DLPLLIB</td>
</tr>
<tr>
<td>DELTA IMS for DBCTL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DELTA PLUS VIRTUAL TERMINAL</td>
<td>DLVCI@00</td>
<td>&amp;DLPTLIB</td>
</tr>
</tbody>
</table>

Accessing the products from an ISPF options menu

Accessing the products from an ISPF options menu requires that you pre-allocate the necessary ISPF data sets to the user.

You must add the following libraries to the TSO logon procedure for each user who requires access to the product(s):

- Load library (ISPLLIB)
- ISPF panel library (ISPPLIB)
- ISPF message library (ISPMLIB)
- ISPF table library (ISPTLIB)

The products contain a hidden panel that allows you to specify many ISPF default product values. The panel is located in member DLPZUSER of the DLPPLIB library. Review the member to customize the ISPF interface default values for the product. Comments are included in the member to assist you.

**Note**

You must change DLPZUSER if you are a licensed ETA customer and want to invoke the ETA CLIST from within DELTA PLUS. For the specific variable that you must change in DLPZUSER.
The following figure shows a sample ISPF/PDF Primary Option Menu with the modifications that are required to access DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL.

Sample modifications to ISPF/PDF Primary Option Menu

```plaintext
%-----------------------  ISPF/PDF PRIMARY OPTION MENU  -----------------
%OPTION  ===>                                                           +
% 0 +ISPF PARMS  - Specify terminal and user parameters
% 1 +BROWSE      - Display source data or output listings
% 2 +EDIT        - Create or change source data
% 3 +UTILITIES   - Perform utility functions
% 4 +FOREGROUND  - Invoke language processors in foreground
% 5 +BATCH       - Submit job for language processing
% 6 +COMMAND     - Enter TSO command or CLIST
% 7 +DIALOG TEST - Perform dialog testing
% C +CHANGES     - Display summary of changes for this release
% D +DELTA PLUS-   IMS DYNAMIC CHANGE FACILITY
% Q +SDSF       - Spool Display and Search Facility
% S +SMP/E      - New Version of SMP
% T +TUTORIAL    - Display information about ISPF/PDF
% X +EXIT       - Terminate ISPF using log and list defaults
%
+Enter%END+command to terminate ISPF.
%
}INIT
HELP = ISR00003
&ZPRIM = YES /* ALWAYS A PRIMARY OPTION MENU */
&ZHTOP = ISR00003 /* TUTORIAL TABLE OF CONTENTS */
&ZHINDEX = ISR91000 /* TUTORIAL INDEX - 1ST PAGE */
}PROC
&ZSEL = TRANS( TRUNC (&ZCMD,'.')
  0,'PANEL(ISPOPTA)'
  1,'PGM(ISRBRO)'
  2,'PGM(ISREDIT)'
  3,'PANEL(ISRUTIL)'
  4,'PANEL(ISRPFA)'
  5,'PGM(ISRJB1) PARM(ISRJPA) NOCHECK'
  6,'PANEL(ISRTSOT)'
  7,'PGM(ISRYXDR) NOCHECK'
C,'PGM(ISPTUTOR) PARM(ISR00005)'
D,'CMD(DLPEXEC MAIN) NEWAPPL(DLP) PASSLIB' (DELTA PLUS)
OR
D,'CMD(DLPEXEC MAIN DBCTL) NEWAPPL(DLP) PASSLIB' (DELTA PLUS for DBCTL)
OR
D,'CMD(DLPEXEC MAIN VT) NEWAPPL(DLP) PASSLIB (DELTA PLUS VIRTUAL TERMINAL)
Q,'PANEL(ZSDSFOPT) NEWAPPL(ISF)'
S,'PGM(GIMISCV) PARM(&ZCMD) NEWAPPL(SMP2)'
T,'PGM(ISPTUTOR) PARM(ISR00000)'
X,'EXIT'
*,?')
```
Limiting access to the products

By default, access to many product functions is unlimited.

To restrict product usage, you must take steps to protect the functions that you want to restrict.

Under most circumstances, you do not have to set security when initially installing the products. Therefore, you may want to defer setting security until you have reviewed the various security methods.

DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL allow you to secure product features through either of the following methods:

- **User access profiles**
  If you decide to secure product features through user access profiles, you must first establish administrator authority to create and change user access profiles. After you establish administrator authority for appropriate users, you can use UPF security to create and maintain user access profiles. For more information about establishing administrator authority and using UPF, see Implementing user access profiles and UPF security (see page 60).

- **A System Authorization Facility (SAF) interface to RACF or an equivalent product**
  For more information about securing product features through a SAF interface, see Implementing a SAF interface to RACF (or equivalent) product (see page 67).

**Note**

If you are going to restrict access to product functions via the SAF security interface, you must define the ACTIVATE resource before SAF will activate. The ACTIVATE resource provides a method to quickly activate and deactivate the interface. Users must have READ access to the ACTIVATE resource to access the product main menu. You should not define the ACTIVATE resource until you define all other resources.

**Warning**
If your site is running ACF2 and you elect not to install the SAF security interface, you must add the following SAFDEF entry to your ACF2 parameters:

```
FUNCRET(4) FUNCRSN(0) ID(product) MODE(IGNORE)
RACROUTE REQUEST=AUTH CLASS=prd#) RETCODE(4)
```

Failure to add this SAFDEF entry may cause you to receive the following error message when attempting to perform any product function:

`BMCprdnnnnnn NOT AUTHORIZED TO USE product`

Adding this SAFDEF entry will ensure that your existing internal product security will be used. If you decide to use the SAF security interface at a later time, you must delete this SAFDEF entry from your ACF2 parameters.

- **TopSecret**
  For more information about implementing TopSecret to secure product features, see Implementing TopSecret (see page 70).

Unless you use one of these methods to control use of product features, access to the products and use of their features is effectively unlimited. The approaches to internal security are mutually exclusive.

The following table lists the internal security modules for DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL. Depending on the type of security that you implement to limit access, link the appropriate module.

<table>
<thead>
<tr>
<th>If you use</th>
<th>Link</th>
<th>Using DLPCNTL member</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSO userID access list</td>
<td>DLPYUID0</td>
<td>DLP#UIDL</td>
</tr>
<tr>
<td>RACF interface</td>
<td>DLPYRCN0</td>
<td>DLP#RSCL</td>
</tr>
<tr>
<td>SAF interface</td>
<td>DLPYSAF</td>
<td>DLP#SAF1</td>
</tr>
</tbody>
</table>

### Implementing user access profiles and UPF security

Use the following procedure to implement user access profiles and UPF security.

⚠️ **Note**

If you are converting from DELTA IMS to DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL, you can use your existing DELTA IMS UPF data set by specifying the name of the data set in the User Profiles data set field in the Global Options. If you currently use customized keyword tables, you can convert them to view profiles. For more information about keyword table conversion, see the product user guide.
By default, user access profiles determine which product features a user is authorized to use on a specific IMS system. The UPF data set is used to maintain user access profiles. A user access profile is the user ID's authorization for an IMSID. All product functions that reference an IMS control region require specification of the control region's IMSID. Before a user may designate an IMSID, a user access profile must exist for the user ID and IMSID combination.

**Note**

The user access profile specifies that the user may access an IMSID during DELTA List processing, IMS command execution, and IMS control region storage display and update. A user access profile also specifies the view profile suffix to be used for DELTA List processing and History File reporting.

Administrator authority is required to create and maintain user access profiles. Unless you establish administrator authority for appropriate users, access to product features is effectively unlimited: all users are authorized to create user access profiles, so all users can authorize themselves to use all product features. BMC recommends that you establish administrator authority for appropriate personnel and restrict the use of product features, as appropriate, by creating user access profiles.

You can establish administrator authority for users with either of the following methods:

- **User ID list**
  You can create a list of user IDs that have administrator authority for creating and modifying user access profiles. Member DLPYUID0 of the DLPSAMP library contains a sample user ID list that you can modify for your facility.
  The following guidelines apply to creating the user ID list:
  - The user ID list allows generic parameters. That is, only the specified characters in the user ID are matched. The DLPSAMP library member provides information about using generic parameters.
  - Specify the most specific user IDs toward the beginning of the table because the first match, rather than the best match, determines administrator authority. BMC recommends that the last entry in the list contain all asterisks for the user ID and deny administrator authority. This ensures that only the users that you specifically identify in the user ID list have authority to create and modify user access profiles.

- **RACF or an equivalent security product**
  You can use RACF or equivalent commands to define the resource and permit users to access it. Member DLPYRCN0 of the DLPSAMP library contains sample statements that you can use.

**Note**
The products issue RACHECK or equivalent macro instructions before permitting a change to the user profile data set. This macro tests for the appropriate attribute for class APPL and resource DELTAIMS. The class and resource names are specified in the CSECT DLPYRCN0, which is distributed in source form in the DLPSAMP library. You can change the CSECT if necessary.

For detailed instructions for establishing administrator authority and creating user access profiles, see To establish administrator authority (see page 62) and To create user access profiles (see page 64).

To establish administrator authority

1. Determine how you want to establish administrator authority for user access profiles:

<table>
<thead>
<tr>
<th>If you want to establish administrator authority through</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user ID list</td>
<td>Step 2 (see page 62)</td>
</tr>
<tr>
<td>RACF or an equivalent security product</td>
<td>Step 3 (see page 63)</td>
</tr>
</tbody>
</table>

2. Establish administrator authority through a list of user IDs.
   a. Specify the user ID and administrator authority.
      Use the $DLPUID macro instruction in member DLPYUID0 of the DLPSAMP library.
      Use the following format:

      $DLPUID userid,update-flag,control-flag

      The following values are valid for update-flag: Y indicates that the user ID should have basic and DELTA List creation authority, and N indicates that the user ID should have only basic access.
      The following values are valid for control-flag: Y indicates that the user ID should have administrator authority, and N indicates that the user ID should not have administrator authority. Unlike RACF, control authority in a user ID list does not imply update authority.
      b. Repeat as needed to establish the required authority for the appropriate user IDs.

   Note

   To ensure that only the users that you identify in the user ID list have authority to specify global options and create user access profiles, BMC recommends that the last entry in the list contain all asterisks for the user ID and deny administrator authority.
c. To implement the user ID list, use JCL similar to that in member DLP#UIDL of the DLPCNTL library to assemble and relink the panel processor module. If you do not use the JCL that is provided with the product to perform this step, ensure that the DLPSAMP library is included in the SYSLIB concatenation for the JCL that you use.

3. Establish administrator authority through RACF or an equivalent security product.
   a. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If your facility uses</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF (any currently-supported version)</td>
<td>No special statements or maintenance are required. Go to Step 3.b (see page 63).</td>
</tr>
<tr>
<td>ACF2</td>
<td>Add the following SAFDEF entry to your ACF2 parameters:</td>
</tr>
</tbody>
</table>

   ```plaintext
   FUNCRET(4) FUNCTION(0) ID(DLP)
   MODE(IGNORE)
   RACROUTE REQUEST=AUTH CLASS=DLP#
   RETCODE(4)
   ```

   This ensures the use of internal security (any of the available approaches). To use the SAF security interface, you must delete this SAFDEF entry.

   b. Use the RACF RDEFINE command (or, for other security products, its equivalent) to define the product to class APPL. You can use RDEFINE to specify as many parameters as required. Following is an example of the RDEFINE command:

   ```plaintext
   RDEFINE APPL DELTAIMS UACC(READ)
   ```

   c. Use the RACF PERMIT command or equivalent to grant administrator authority to user IDs, as necessary. Following is an example of the PERMIT command:

   ```plaintext
   PERMIT DELTAIMS CLASS(APPL) ID(userid) ACCESS(CONTROL)
   ```

   In this example, the userid is also granted authority to create DELTA Lists since RACF control authority implies update authority.

d. Optionally, issue the RACF PERMIT command or equivalent to grant update authority for creation of DELTA Lists. For example:

   ```plaintext
   PERMIT DELTAIMS CLASS(APPL) ID(userid) ACCESS(CONTROL)
   ```

   e. Repeat steps Step 3.b (see page 63), Step 3.c (see page 63), and Step 3.d (see page 63) as needed to establish the required authority for the appropriate user IDs.
f. To implement the new RACF or equivalent security information, use JCL similar to that in member DLP#RSCL of the DLPCNTL library to relink the panel processor module.

⚠️ **Note**

This job assembles and links DLPSAMP library member DLPYRCN0, which specifies class APPL and resource DELTAIMS. The latter name was chosen for ease of migrating DELTA IMS installations to DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL.

To create user access profiles

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type 4 in the selection field and press Enter. The Administration Menu is displayed.
3. Type 9 in the selection field and press Enter. The User Access Profiles panel is displayed.

**User Access Profiles (UPF) panel**

<table>
<thead>
<tr>
<th>IMSID/UserId</th>
<th>Group</th>
<th>IMS</th>
<th>Last Modification</th>
<th>Exec/Chk</th>
<th>IMS</th>
<th>Storage</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ DLAID</td>
<td>IMSA</td>
<td>N</td>
<td>07/06/04 12:00:42</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>_ DLPID</td>
<td>IMSB</td>
<td>M</td>
<td>07/06/04 12:01:13</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

⚠️ **Note**
If you use SAF security, you will only need to update the view profile suffix information in the UPF data set.

The following fields are available on this panel:

**Data set name:**
The name of the partitioned data set that contains all user access profiles. Each time you access this panel, the data set name defaults to the user profile data set name that is contained in DLP$GBL0.A.

Type D in the action field to delete an entry.

**Userid**
Displays a specific user ID or masking pattern that defines a user or group of users for which access to the product is desired.

The Userid and IMSID/Group fields are used together to determine system access and are searched in the order listed. Specific IDs will be matched before generic IDs.

To change this field, you must delete the entire entry using the D line command, and then reinsert it using the INSERT command.

**IMSID/Group**
Displays a specific IMSID or a masking pattern that can allow the user to access one or more IMSIDs.

The Userid and IMSID/Group fields are used together to determine system access and are searched in the order listed. Specific IDs will be matched before generic IDs.

To change this field, you must delete the entire entry using the D line command, and then reinsert it using the INSERT command.

**DELTA List Exc**
Type Y or N to indicate whether the user can execute a DELTA List.

**DELTA List Chk**
Type Y or N to indicate whether the user can check a DELTA List.

**Exec IMS Cmds**
Type Y or N to indicate whether the user can issue IMS operator commands. This variable limits IMS commands that are issued from the Execute IMS Command panel only.

**Upd IMS Parms**
Type Y or N to indicate whether the user can update the virtual terminal options. Update Parms authority is required to perform the following actions:

- Edit and refresh IMSID and Group options
- Add an IMSID to a group log
- Run the Log and History File SYSGEN Date Change utility
- Obtain the status of, purge, recover, or format the Log and History files
- Refresh CPU ID and TSS look-aside buffers

**IMS Storage Dsply**
Type Y or N to indicate whether the user can display IMS control region storage.

**IMS Storage Zap**
Type Y or N to indicate whether the user can apply zaps to IMS control region storage.

**Warning**

Enabling the Storage Dsply and Storage Zap options permits the product to display storage contents within the IMS address space at the TSO terminal. If misused, the Storage Dsply option can compromise data confidentiality. Users who can display IMS...
storage can also, if authorized, use the product to alter (or zap) storage. The product imposes no restrictions over the z/OS operating system or the data or addresses zapped. If misused, a loss of system integrity could result.

View Profile Suffix
Under UPF security, DELTA List edit, check, and execute operations and DELTA Log reports are always secured by a view profile with a name of the form DLAKWTxx (for DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL) or DDCKWTnn (for DELTA PLUS for DBCTL). Type the correct suffix in this field. See the product user guide for more information about view profiles, DELTA List editing, checking, and execution, and conversion of DELTA IMS keyword tables to view profiles.

To insert a new entry, type INSERT on the Command line and press Enter. The following figure shows the INSERT command syntax.

```
INSERT
useridptrn
imsidorgroupptrn
```

The useridptrn operand specifies a user ID or pattern, and the imsidorgroupptrn operand specifies an IMSID or group or a pattern. Patterns use an asterisk (*) as the wildcard character. Generally, each wildcard character matches exactly one character.

⚠️ Note
The DELTA IMS and DELTA PLUS (and DELTA PLUS VIRTUAL TERMINAL) UPF editors handle patterns that are destined for theIMSID/Group field differently. If an inserted pattern ends with a wildcard character, then that character will be extended to the length of the field under DELTA IMS. If an IMSID or group matches the leading characters of a shorter length pattern that ends with a wildcard, then a match will occur. Thus, new records inserted under DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL could match earlier in the collating sequence than records inserted under DELTA IMS.

When falling back from DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL to DELTA IMS, records with short IMSID/Group values may continue to exist. DELTA IMS will not match an IMSID or group to a shorter pattern, but will match an equal length or longer pattern whose excess characters are wildcards. Thus, records inserted by DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL could be ignored by DELTA IMS.

If one or both INSERT command operands were not specified, the Insert User Access Profile pop-up window is displayed.

**Insert User Access Profile pop-up window**
The following fields are available on this panel:

**Userid or mask**
Type a specific user ID or masking pattern to define a user or group of users. This field will be populated from the corresponding INSERT command operand.

**IMSID/Group or mask**
Type a specific IMSID or group name, or a pattern.

### Implementing a SAF interface to RACF (or equivalent) product

The SAF interface allows you to use RACF or an equivalent product to secure all product features.

By defining a special security class and defining resources to this class, you can activate the SAF interface and specify the product features that are secured. You can then allow use of product features by giving users READ authority for the appropriate resources. In a RACF environment, any product features that are not defined in the security class through the appropriate resource name are not secured and can be used by anyone who initiates a product session. For product features that provide edit and browse capabilities, UPDATE authority is required to access edit, for which browse capability will be assumed.

⚠️ **Note**

This approach to internal security is an alternative to the use of user access profiles (skip this task if you secure the product through user profiles).

### To secure product features through the SAF interface

1. Add a product class to the RACF or equivalent class descriptor table that is identified in macro ICHERCDE.
   a. If you cannot use class DLP# because of class naming conventions at your site or because the class already exists, use the JCL in member DLP#SAF1 of the DLPCNTL library to change the class name that the product expects the security product to use. Otherwise, add class DLP# to the class descriptor table.
   b. You must specify the following parameters for the class definition:

```
MAXLNTH=100
```
2. Add the product class to the RACF or equivalent class router table that is identified in macro ICHRFRTB.
3. Specify the product features that will be secured by defining the appropriate resources to the product class.

⚠️ **Warning**

Under RACF, anyone who invokes a product session can use product features that you do not secure.

The following table identifies the functions that you can secure. The table also provides each feature’s resource name. Within the table:
- **target** = four-character IMSID or group name
- **cmd** = three-character IMS command abbreviation
- **vname** = one- to eight-character View Profile name
- **name** = one- to eight-character member name

**SAF resources for DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL functions**

<table>
<thead>
<tr>
<th>Product function</th>
<th>SAF resource</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td>Activate</td>
<td>ACTIVATE</td>
<td>Yes</td>
</tr>
<tr>
<td>Log/History File SYSGEN Date Change Utility</td>
<td>DLP.ADMIN.CHGDATE</td>
<td>Yes</td>
</tr>
<tr>
<td>Global Options</td>
<td>DLP.ADMIN.GLOBAL</td>
<td>Yes</td>
</tr>
<tr>
<td>IMSID Options</td>
<td>DLP.ADMIN.IMSID</td>
<td>Yes</td>
</tr>
<tr>
<td>Group Options</td>
<td>DLP.ADMIN.GROUP</td>
<td>Yes</td>
</tr>
<tr>
<td>User Profile</td>
<td>DLP.ADMIN.UPF</td>
<td>Yes</td>
</tr>
<tr>
<td>View Profile Edit</td>
<td>DLP.ADMIN.VIEWPROF.vname</td>
<td>Yes</td>
</tr>
<tr>
<td>View Profile Use</td>
<td>DLP.VIEWPROF.vname</td>
<td>Yes</td>
</tr>
<tr>
<td>Product Authorization</td>
<td>DLP.ADMIN.PRODAUTH</td>
<td>Yes</td>
</tr>
<tr>
<td>DELTA List Check/Execute</td>
<td>DLP.target:DELTALST.RUN</td>
<td>Yes</td>
</tr>
<tr>
<td>DELTA List Browse/Edit</td>
<td>DLP.DELTALST.name</td>
<td>Yes</td>
</tr>
<tr>
<td>IMS Command Interface</td>
<td>DLP.target:COMMAND.cmd</td>
<td>Yes</td>
</tr>
<tr>
<td>Log Report</td>
<td>DLP.target:LOG.REPORT</td>
<td>Yes</td>
</tr>
<tr>
<td>Product function</td>
<td>SAF resource</td>
<td>Supports</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update</td>
</tr>
<tr>
<td>Log Status</td>
<td>DLP.target.LOG.STATUS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Log Purge</td>
<td>DLP.target.LOG.PURGE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Log Recover</td>
<td>DLP.target.LOG.RECOVER</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Log Format</td>
<td>DLP.target.LOG.FORMAT</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>History Report</td>
<td>DLP.target.HISTORY.REPORT</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>History Status</td>
<td>DLP.target.HISTORY.STATUS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>History Purge</td>
<td>DLP.target.HISTORY.PURGE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>History Recover</td>
<td>DLP.target.HISTORY.RECOVER</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>History Format</td>
<td>DLP.target.HISTORY.FORMAT</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Storage Display/Zap</td>
<td>DLP.target.STORAGE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes (Zap)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Display)</td>
</tr>
<tr>
<td>Add IMS to Group Log</td>
<td>DLP.ADMIN.ADDIMS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Remove IMSID from Group Log/History File</td>
<td>DLP.ADMIN.REMOVIMS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Convert Log to Stage 1</td>
<td>DLP.target.CONVERT.LOG.STAGE1</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Convert Log to DELTA List</td>
<td>DLP.target.CONVERT.LOG.DELTALST</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Convert DELTA List to Stage 1</td>
<td>DLP.CONVERT.DELTALST.STAGE1</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>IMSID and Group Options Refresh</td>
<td>DLP.target.REFRESH.OPTIONS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>CPU ID Refresh</td>
<td>DLP.target.REFRESH SECURITY</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Variable Definition Edit</td>
<td>DLP.ADMIN.VARDEF.name</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes (Edit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Browse)</td>
</tr>
<tr>
<td>Variable Definition Use</td>
<td>DLP.VARDEF.name</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

**ALL REMAINING FUNCTIONS APPLY ONLY TO DELTA PLUS VIRTUAL TERMINAL**

<table>
<thead>
<tr>
<th>Product function</th>
<th>SAF resource</th>
<th>Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update</td>
</tr>
<tr>
<td>Back Up TSS Data Set</td>
<td>DLP.TSS.BACKUP</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Define TSS Table</td>
<td>DLP.TSS.DEFINE.name</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>TSS Table Browse/Edit</td>
<td>DLP.TSS.EDIT.name</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>TSS Table Test/Search-Modify</td>
<td>DLP.TSS.EDIT.name</td>
<td>Yes (Test)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes (Search-Modify)</td>
</tr>
<tr>
<td>Format TSS Data Set</td>
<td>DLP.TSS.FORMAT</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Load TSS Table(s)</td>
<td>DLP.TSS.LOAD.name</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Remove TSS Table(s)</td>
<td>DLP.TSS.REMOVE.name</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Reorganize TSS Data Set</td>
<td>DLP.TSS.REORG</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Product function</td>
<td>SAF resource</td>
<td>Supports</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Status of TSS Data Set</td>
<td>DLP.TSS.STATUS</td>
<td>Read Yes Update No</td>
</tr>
<tr>
<td>Unload TSS Table(s)</td>
<td>DLP.TSS.UNLOAD.name</td>
<td>Read Yes Update No</td>
</tr>
<tr>
<td>Refresh TSS In-Storage Buffers</td>
<td>DLP.target.REFRESH.TSS</td>
<td>Read Yes Update No</td>
</tr>
<tr>
<td>Display of VIRTUAL TERMINAL</td>
<td>DLP.target.VTSTATS</td>
<td>Read Yes Update No</td>
</tr>
</tbody>
</table>

4. Give users read authority for the resources (product features) that they need to use. For features that provide browse and edit capabilities, specify READ authority for browse and UPDATE authority for edit. Browse capability will be assumed for users with edit capability.

5. Define the ACTIVATE resource to the product class. When you define this resource, RACF or an equivalent security product restricts access to the product features that you specified, and user access profile checking is disabled.

**Implementing TopSecret**

You can implement SAF security with TopSecret to protect every function within DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL.

To implement SAF security checking with TopSecret, perform the following steps:

1. Contact your TopSecret administrator to add a new SAF class.
   The SAF class defines the functions that are to be protected. The default class name is DLP#. However, if you want to change the class name, you can edit member DLPYSAF of the DLPSAMP library (as documented in the member). Run job DLP#SAF1 from the DLPCNTL library to update the DLPU007 module in the load module library. The class name supplied in member DLPYSAF of the DLPSAMP library will be the class name that is used for SAF security checking.

2. Define the class in the TopSecret Resource Definition Table (RDT). Issue the following TSS command:

   ```plaintext
   TSS ADD(RDT) RESCLASS(DLP#) RESCODE(hex_code) MAXLEN (100) [ACLST(access_level_list)] [DEFACC(default_access_level)]
   ```

   Your TopSecret administrator should be able to determine the RESCODE, ACLST, and DEFACC.

3. Determine which functions within the product that you want to restrict.
   For example, to restrict access to the Convert-History-to-Stage1-Macros Utility, issue the following TSS command:

   ```plaintext
   TSS ADD(DLP#) RESCLASS(DLP.*.CONVERT,HISTORY.STAGE1) DEFACC(ALL)
   ```
To protect a specific function, you must define the associated resource name within the product class. A user must have at least READ access to a resource to have access to the function. If the user who is requesting the function does not have READ access to the resource, the request will be rejected.

Any function that is not protected (the associated resource name is not defined within the product class) can be accessed by any user requesting the function. If a user has UPDATE access, READ access is also assumed.

4. Issue the following TSS commands to define the ACTIVATE resource within the class, where `deptims` is the owner of the resources:

```
TSS ADD(deptims) DLP#(ACTIVATE)
```

For example, the owner could be a department or a user.

```
TSS PERMIT(ALL) DLP#(ACTIVATE) ACC(READ)
```

You must define the ACTIVATE resource before you can activate the SAF security interface. This feature allows you to quickly activate and deactivate the interface. Users must have READ access to the ACTIVATE resource to access the product ISPF interface or batch functions. You should not define the ACTIVATE resource until you have defined all other resources.

5. Log on to the ISPF interface and issue the SAF command. The panel will display whether SAF is active.

6. Press F1. The following information displays:

```
SAF security is enabled for product, class class_name.
```

Ensure that `class_name` matches the SAF class that you defined.

7. To restrict individual users, issue the following TSS command:

```
TSS PERMIT(userid) RESCLASS(DLP.*.CONVERT.HISTORY.STAGE1) ACCESS(NONE)
```

---

Setting global options in DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL

This section describes the procedures for setting global options.
Use global options to specify parameters that govern product operations throughout your site, regardless of IMS system. You must review and save the global options if you are performing an initial installation of DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL.

DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL consist of various elements that are associated through VTAM and normal IMS inter-region communication. You must specify certain parameters to keep these elements operating according to the standards at your site. Global options apply to all TSO/ISPF sessions, batch functions, BMCXLINK, and all control regions that the products service. When you create or change global options, load module DLP$GBL0 is link-edited to your product options library.

**Note**

- When global options are changed, other users must re-enter the product to obtain the revised options. For proper operation, you should recycle BMCXLINK.
- If you have an existing DELTA IMS global options module (DLA$GBL0), certain global options field values can be copied from DLA$GBL0. For more information, see the conversion appendices in the product user guide.

**To set global options**

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type 4 in the selection field and press Enter. The Administration Menu is displayed.
3. Type 1 in the selection field and press Enter. The Global Options Entry panel is displayed.

**Global Options Entry panel**

```
Menu  Options  Help
-------------------------------------------------------------------------------
prd                         Global Options Entry
Command ===> _________________________________________________________________

Specify the library containing the Global Options.
Global Options library  . 'prd.APF.LOAD'

Specify additional libraries in which to save Options (if desired).
Save library 1  . . . . . ______________________________________________
Save library 2  . . . . . ______________________________________________
```
4. In the **Global Options library** field, type the data set name of the library in which the global options module will reside.

   ![Note]
   
   The product interface obtains the global options module from one of the following sources:
   - TSO logon procedure //STEPLIB concatenation
   - product CLIST ISPLLIB concatenation

5. *(optional)* If your installation stores the global options module in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the global options module in the **Save library 1** field and press **Enter**.

   ![Note]
   
   If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

The Edit Global Options panel is displayed.

**Edit Global Options panel**

The following fields are available on this panel:
VTAM User Session ACBNAME prefix
Specify the four-character ACBNAME prefix from the VTAM definition statements that were created during the product installation.
The BMCXLINK ACBNAMEs that are used in the VTAM definition statements must be of the format ppppnnnn, where pppp is the four-character prefix specified in this field, and nnnn is the next available sequential number starting with 0001.
The default value for this field is DLPU.

DASD unit name for temporary files
Specify the esoteric DASD unit name that the product Log and History File functions use to allocate work files and temporary report files during sorts.
The default value for this field is SYSALLDA.

Trace table dynamic dump sysout class
Specify the sysout class to be used if the internal trace table appears in any abend dumps.
This class is also used if the table must be printed on demand.
The default value for this field is A.

Request status check time interval
Specify the time interval, in seconds, after which the product will provide a status on any outstanding requests. The product periodically responds to the BMCXLINK user session while processing a request for that session so that the user stays informed of the request processing status.
The default value for this field is 10 seconds.

Routing code
Type the WTO message routing code that the product and BMCXLINK will use. BMCXLINK issues WTO messages any time significant events occur. Use the WTO routing code to direct these messages to selected consoles.
BMC recommends that you use the default value of 11.
For information about other routing codes, see IBM publication MVS/ESA Routing and Descriptor Codes or z/OS MVS System Messages.

Descriptor code
Type the WTO message descriptor code that the product and BMCXLINK will use.
BMCXLINK issues WTO messages any time significant events occur. You can suppress these messages depending on the WTO message descriptor code specified.
BMC recommends that you use the default value of 7.
For information about other descriptor codes, see IBM publication MVS/ESA Routing and Descriptor Codes or z/OS MVS System Messages.

Translate all messages to uppercase
Type a / in the selection field to translate product-generated messages to uppercase.
Otherwise, messages are generated in mixed case.
This option affects only the messages that are displayed on the console or in batch. It does not affect ISPF messages unless the message comes from BMCXLINK.

Message number prefix
Select a product message prefix.
Type 1 in the selection field to prefix the product error message with the BMCDLP prefix (for example, BMCDLP123456E).
Type 2 in the selection field to prefix the product error message with the DLP prefix (for example, DLP123456E).
Type 3 in the selection field to prefix the product error message with the BMC prefix (for example, BMC123456E).

View Profile library
Specify the name of the data set that will store the View Profiles which allow you to customize element fields in the ISPF interface.
For information about allocating this data set, see Allocating new data sets (see page 104).

Variable Definition library
Specify the name of the data set that will store the Variable Definition Sets which allow you to customize values for element fields in the ISPF interface.
For information about allocating this data set, see Allocating new data sets (see page 104).

User Profiles data set
Specify the name of the data set that will store the user access profiles that provide internal product security. This data set is allocated during initial installation.
For information about allocating this data set, see Allocating new data sets (see page 104).

Select user id type for batch execution (selection field)
Type the option number in the selection field to indicate which user ID is recorded in the Log and History File when a DELTA List check or execute is initiated. Possible values are:
- 1 Use the active user id
- 2 Use the last-update user id
The default value for this field is 1.

6. Press F3 to save changes to the global options.

Setting IMSID options when installing DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL.

This section describes the procedures for setting IMSID options.
You should set IMSID options if you are performing an initial installation of DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL.

You must create IMSID basic options for each control region that the products service. For more information, see To set IMSID options (see page 79).

For the products to access an IMS system, you must define the system to the products with a set of IMSID options. When you create or change IMSID options, the load module DLP#iii (where iii is the IMSID) is link-edited to your product options library.

You can create a new IMSID by using the product defaults or by copying the options for a new IMSID from an existing IMSID. For more information, see To create a new IMSID (see page 76).

DELTA PLUS VIRTUAL TERMINAL includes IMSID options that are not available with DELTA PLUS. For additional IMSID options that you can set for DELTA PLUS VIRTUAL TERMINAL, see Setting virtual terminal IMSID options (see page 109).

⚠️ **Note**
BMC recommends the following regarding the IMSID options modules:

- Use the APF-authorized library to provide both ISPF and IMS with access to the IMSID options modules.
- Do not use a LINKLIST library to store the IMSID options modules.
- Save IMSID options modules in the same library with the global and Group options (if used) modules.
- If you have an existing DELTA IMS IMSID options module (DLA#iii), certain IMSID options module fields can be copied from DLA#iii. For more information, see the conversion appendices in the product user guide.

**To create a new IMSID**

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type 4 in the selection field and press **Enter**. The Administration Menu is displayed.
3. Type 2 in the selection field and press **Enter**. The IMSID/Group Options Entry panel is displayed.
3. Choose a selection:
   1. Edit IMSID Options
   2. Edit Group Options

Specify Options information:
   Options library . . . . . 'ABC.DLP.OPTIONS.LOAD'
   IMSID or Group . . . . . . ___ (blank for selection list)

Specify additional libraries in which to save Options (if desired):
   Save library 1 . . . . .
   Save library 2 . . . . .

4. Determine the method that you want to use to create the new IMSID:

<table>
<thead>
<tr>
<th>If you want to create the new IMSID by</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the product defaults</td>
<td>Step 5 (see page 77)</td>
</tr>
<tr>
<td>Copying options from an existing IMSID</td>
<td>Step 6 (see page 77)</td>
</tr>
</tbody>
</table>

5. Type the name of the new IMSID in the IMSID or Group field and press Enter.
   The IMSID options will be populated from internal product defaults.

6. Type the name of the new IMSID in the IMSID or Group field and press Enter.
   If you are installing DELTA PLUS, the DELTA PLUS Edit IMSID Options panel is displayed.
   If you are installing DELTA PLUS VIRTUAL TERMINAL, the DELTA PLUS VIRTUAL TERMINAL Edit IMSID Options panel is displayed.

   **DELTA PLUS Edit IMSID Options panel**

<table>
<thead>
<tr>
<th>DELTA PLUS VT</th>
<th>IMSID Options - Basic Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ===&gt;</td>
<td></td>
</tr>
</tbody>
</table>

   IMSID . . . . . . . . . . : IMSA
   More:               +

   Display/Zap Options. Select if desired.
   / Allow IMS storage displays
   / Allow IMS storage zaps

   Save Options. Select if desired.
   _ Copy IMSID Options to an IMS STEPLIB library when saved
     IMS STEPLIB library . . .

   XRF/FDR Alternate IMSID . . . ___ (If changed, IMS restart is required)
XCF Group (optional) . . . . ____ (If changed, IMS cold-start is required)

IMS Restart Options (if XCF Group specified above). Select if desired.
  Do not issue WTOR for coordinated request errors

DELTA PLUS VIRTUAL TERMINAL Edit IMSID Options panel

File  Edit  Refresh  Options  Help
---------------------------------------------------------------
DELTA PLUS VT   Edit IMSID Options
Command ===> 

IMSID . . . . . . . . . . : WXC5

IMSID options. Choose a selection.
  1. Basic       - Info required for DELTA PLUS VT operation
  2. VT Limits   - Limits for virtual terminals
  3. VT Options  - Options for virtual terminals
  4. VT TSS      - TSS tables for virtual terminals
  5. VT Logon    - Logon for virtual terminals
  6. VT Signon Bypass - Signon Bypass for virtual terminals
  7. VT Signon   - Signon for virtual terminals
  8. Extended Options - DELTA PLUS VT extended options

To update IMSID options in the control region

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type 4 in the selection field and press Enter. The Administration Menu is displayed.
3. Type 5 in the selection field and press Enter. The Refresh Menu is displayed.
   Refresh Menu
4. Type 1 in the selection field.
5. In the **IMSID or Group** field, type the IMSID that you want to update and press Enter.
The Confirm Options Refresh pop-up window is displayed.
6. Type 1 in the selection field and press **Enter**.
The product refreshes the IMSID options.

**To set IMSID options**

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in [Accessing the products from an ISPF options menu (see page 57)](#) or through the CLIST that you created in [Accessing the products from a CLIST (see page 57)](#).
The Main Menu is displayed.
2. Type 4 in the selection field and press **Enter**.
The Administration Menu is displayed.
3. Type 2 in the selection field and press **Enter**.
The IMSID/Group Options Entry panel is displayed.
4. Type 1 in the selection field.
5. Type the data set name of the library in which the IMSID options module (DLP#iii) will reside in the **Options library** field.
For information about allocating this data set, see [Allocating new data sets (see page 104)](#).
6. Perform the appropriate action.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicate a specific IMSID for the IMS system that you want to customize or access.</td>
<td>Type the IMSID of the IMS system in the <strong>IMSID or Group</strong> field. This action is required for the first set of IMSID options.</td>
</tr>
<tr>
<td>Choose an IMSID that you want to customize or access from a list of IMSIDs.</td>
<td>Leave the <strong>IMSID or Group</strong> field blank.</td>
</tr>
</tbody>
</table>

7. *(optional)* If your installation stores IMSID/Group options modules in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the IMSID options modules in the **Save library 1** field and press **Enter**.
If you typed a specific IMSID in the **IMSID or Group** field, the Edit IMSID Options panel is displayed. Go to Step 9 (see page 80).

If you left the **IMSID or Group** field blank, the Edit IMSID Options – List panel is displayed, allowing you to select an IMSID. Go to Step 8 (see page 80).

**Figure 5. Edit IMSID Options - List panel**

8. Perform one of the following actions:
   - Create a new IMSID options module by typing `S newimsid` on the **Command** line.
   - Modify an existing set of options by typing `S next` to an existing IMSID.

   Press **Enter**.

   If you are installing DELTA PLUS, the DELTA PLUS Edit IMSID Options panel is displayed. Go to Step 9 (see page 80).
   If you are installing DELTA PLUS VIRTUAL TERMINAL, the DELTA PLUS VIRTUAL TERMINAL Edit IMSID Options panel is displayed. Go to Step 9 (see page 80).

9. Type **1** in the selection field and press **Enter**.
   The IMSID Options – Basic Options panel is displayed. The fields on this panel are the same as the fields on the DELTA PLUS Edit IMSID Options panel.
   The following fields are available on this panel:

   **IMSID**
   The IMSID of the options module that you selected.

   **IMS Version or release level**
   Type the IMS version and release for the IMSID. Possible values are:
   - IMS Version 12.1
You can specify an IMS level for each IMS system that uses the product. The products can support a combination of IMS systems.

**Allow IMS storage displays**
Type a / in the selection field to enable the storage display feature for this IMS system. You can use internal security to restrict usage of this feature.

**Allow IMS storage zaps**
Type a / in the selection field to enable the storage alteration (zap) feature for this IMS system. The storage zap feature is a powerful tool for correcting problems within the IMS system. However, you should use internal security to restrict usage of this feature.

**Copy IMSID options to an IMS STEPLIB library when saved**
Type a / in the selection field to copy IMSID options modules to an IMS //STEPLIB library when the module is saved in the options library.

If you select this option, you must specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region in the IMS STEPLIB library field.

**IMS STEPLIB library**
Specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region.

If your installation stores IMSID options modules in separate libraries for use by ISPF and IMS, you should complete this field. If both ISPF and IMS use the same library, this field is optional.

**XRF/FDR Alternate IMSID**
Specify the IMSID of the IMMSGEN-defined XRF alternate system or the IMSID of the FDR control region.

For information about enabling the FDR feature, see Enabling the FDR feature (DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL) (see page 82).

**XCF Group**
Specify the name of the Group to which this IMS system belongs. This field is optional because an IMS system does not have to belong to a Group.

Do not issue WTOR for coordinated request errors

Type a / in the selection field to ensure that the WTOR (write to operator with reply) message BMC186124A Errors applying new request from Log, should restart continue? Reply 'Y' or 'N' is not issued at IMS restart if a coordinated request fails.

Reply Y or N for any new coordinated requests that have errors at restart. Error messages are still issued for coordinated request errors.

**BMCXLINK task network LUNAME**
Type a network LUNAME for the BMCXLINK VTAM subtask. The LUNAME that you specify MUST match the LUNAME that is specified in the PARM field of the BMCXLINK task. The default value for this field is DLPALINK.

**Primary Log**
Type the data set name of the primary Log data set. You must cold-start IMS for this change to take effect.

**Secondary Log**
Type the data set name of the secondary Log data set. You must cold-start IMS for this change to take effect.

**Primary History File**
Type the data set name of the primary History File data set. You must restart IMS for this change to take effect.

**Secondary History File**
Type the data set name of the secondary History File data set. You must restart IMS for this change to take effect.

**Write IMS commands to History File**
Type a / in the selection field to send IMS operator commands that are issued from a DELTA List or from the Execute IMS Command panel to the History File.

**(optional) Primary Repository**
Type the name of the primary DELTA PLUS Repository data set.

**(optional) Secondary Repository**
Type the name of the secondary DELTA PLUS Repository data set.

10. Press **F3** to save changes to the IMSID options.

---

**Note**

If you specified an existing IMSID in the **XRF/FDR Alternate IMSID** field, the Confirm Delete pop-up window is displayed before the IMSID options are saved. Type 1 in selection field and press **Enter** to delete the existing options for the IMSID previously specified in the **XRF/FDR Alternate IMSID** field. This selection also makes the IMSID that is specified in the **XRF/FDR Alternate IMSID** field the alternate for the IMSID that you are editing.

---

**Enabling the FDR feature (DELTA PLUS and DELTA PLUS VERTUAL TERMINAL)**

You must complete the following steps to enable the functionality of the FDR feature.

1. Add the product library to the STEPLIB for the FDR region.
2. Ensure that the ACBLIB in the FDR region is the same as in the control region.
3. Verify that the product is licensed on the CPU where the FDR region resides.
4. Specify the IMSID of the FDR region in the **XRF/FDR alternate IMSID** field when you are setting the IMSID basic options for the primary IMSID options module.
5. When you save your IMSID options, the product automatically creates two IMSID options modules. The primary IMSID options module is named DLP#i iii (where iii is the IMSID of your primary system). The second IMSID options module is named DLP#f fff (where fff is the IMSID of the system where the FDR region resides). The product creates these modules automatically to ensure that they are always synchronized.

**Warning**

Never manually edit the IMSID options module for your FDR region. To avoid potential errors, the options for the primary IMSID options module and the FDR region IMSID options module must not conflict.

### Setting Group options

This section describes the procedures for setting Group options.

Group options allow you to treat a user-defined group of IMS systems as one IMS system. A group of IMS systems would typically be an IMS Datasharing Group, IMS Shared Queues Group, or a group of logically related or duplicated IMS systems. When you create or change Group options, the load module DLPZg ggg is link-edited to your options library.

**Note**

Group options are NOT required.

Once you have saved the Group options module, you will have to restart IMS for the changes to take effect. If you perform a Group options REFRESH, the only changes that will take effect are the IMS command options.

You can create a new Group by using the product defaults or by copying the options for a new Group from an existing Group. For more information, see To create a new Group (see page 84).

**Note**

When you are choosing a name for your Group options, be sure that you do not duplicate the name used for existing IMSID options. If you duplicate the IMSID options name for your Group options name, the product will not find the Group options because it will locate the IMSID options first.

BMC recommends the following regarding the Group options module:
To create a new Group

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).
   The Main Menu is displayed.
2. Type 4 in the selection field and press Enter.
   The Administration Menu is displayed.
3. Type 2 in the selection field and press Enter.
   The IMSID/Group Options Entry panel is displayed.
4. Determine the method that you want to use to create the new Group:

<table>
<thead>
<tr>
<th>If you want to create the new Group by</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the product defaults</td>
<td>Step 5 (see page 84)</td>
</tr>
<tr>
<td>Copying options from an existing Group</td>
<td>Step 6 (see page 84)</td>
</tr>
</tbody>
</table>

5. Type the name of the new Group in the IMSID or Group field and press Enter.
   The Group options will be populated from internal product defaults.
6. Type the name of the new Group in the IMSID or Group field and press Enter.
   The Edit Group Options panel is displayed.

   **Edit Group Options panel**

   ----- File Edit Refresh Format Options Help
   -------------------------------
   Command ==>
   
   Group name . . . . . . . : IMSA

   BMCXLINK task network LUNAME  DLPALINK

   DELTA PLUS VT Log Data Set Names.
   Primary Log . . . . . . . 'DLP.PRI.LOG'
   Secondary Log . . . . . . . 'DLP.SEC.LOG'

   DELTA PLUS VT History File Data Set Names.
   Primary History File . . . 'DLP.PRI.HIST'
   Secondary History File . . . 'DLP.SEC.HIST'
Command Options. Select if desired.
- Write IMS commands to history file

Execution Options. Select if desired.
- Allow coordinated requests even if no IMS is active in group

7. Type **COPY name** on the **Command** line (where *name* is the name of the existing Group from which you want to copy the Group options) and press **Enter**.
The new options will be copied from the existing Group.

**To update Group options in the control region**

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).
The Main Menu is displayed.
2. Type **4** in the selection field and press **Enter**.
The Administration Menu is displayed.
3. Type **5** in the selection field and press **Enter**.
The Refresh Menu is displayed.
4. Type **1** in the selection field.
5. In the **IMSID or Group** field, type the name of the Group that you want to update and press **Enter**.
The Confirm Options Refresh pop-up window is displayed.
6. Type **1** in the selection field and press **Enter**.
The product refreshes the Group options.

**To set Group options**

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).
The Main Menu is displayed.
2. Type **4** in the selection field and press **Enter**.
The Administration Menu is displayed.
3. Type **2** in the selection field and press **Enter**.
The IMSID/Group Options Entry panel is displayed.
4. Type **2** in the selection field.
5. Type the data set name of the library in which the Group options module (DLPZgigg) resides in the **Options library** field.
6. Perform the appropriate action:
Activity | Action
--- | ---
Indicate a specific Group that you want to customize or access. | Type the name of the Group in the **IMSID or Group** field.
Choose a Group that you want to customize or access from a list of Groups. | Leave the **IMSID or Group** field blank.

7. **(optional)** If your installation stores IMSID/Group options modules in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the Group options modules in the **Save library 1** field. If ISPF, the control region, and BMCXLINK use the same library, this field is optional.

![Note]

If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

Press **Enter**.

<table>
<thead>
<tr>
<th>Previous action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>You typed a specific Group name in the <strong>IMSID or Group</strong> field.</td>
<td>The Edit Group Options panel is displayed. Go to <strong>Step 9</strong> (see page 86).</td>
</tr>
<tr>
<td>You left the <strong>IMSID or Group</strong> field blank.</td>
<td>The Edit Group Options - List panel is displayed so that you can select a group. Go to <strong>Step 8</strong> (see page 86).</td>
</tr>
</tbody>
</table>

8. Type **S** next to the Group that you want to customize or access and press **Enter**.
The Edit Group Options panel is displayed.
9. Specify the Group options.
The following fields are available on this panel:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group name</strong></td>
<td>The name of the Group that you are creating or modifying. This is not an editable field.</td>
</tr>
<tr>
<td><strong>BMCXLINK task network LUNAME</strong></td>
<td>Type a network LUNAME for the BMCXLINK VTAM subtask. The LUNAME that you specify MUST match the LUNAME that is specified in the PARM field of the BMCXLINK task. The default value for this field is <strong>DLPALINK</strong>.</td>
</tr>
<tr>
<td><strong>Primary Log</strong></td>
<td>Type the name of the primary Log data set. For this change to take effect, you must cold-start all IMS systems that are included in the Group.</td>
</tr>
<tr>
<td><strong>Secondary Log</strong></td>
<td>Type the name of the secondary Log data set. For this change to take effect, you must cold-start all IMS systems that are included in the Group.</td>
</tr>
<tr>
<td><strong>Primary History File</strong></td>
<td>Type the name of the primary History File data set. For this change to take effect, you must cold-start all IMS systems that are included in the Group.</td>
</tr>
<tr>
<td><strong>Secondary History File</strong></td>
<td>Type the name of the secondary History File data set. For this change to take effect, you must cold-start all IMS systems that are included in the Group.</td>
</tr>
</tbody>
</table>
Write IMS commands to history file  
Type a \ in the selection field to send IMS operator commands that are issued from a DELTA List or from the Execute IMS Command panel to the History File.

Allow coordinated requests even if no IMS is active in group  
Type a \ in the selection field to allow coordinated requests even if no IMS is active in the group. The Log will be updated with the requests. You need to restart BMCXLINK to apply these requests.

Copy Group Options to an IMS STEPLIB library when saved  
Type a \ in the selection field to copy Group options modules to an IMS //STEPLIB library when the module is saved in the options library. If you select this field, you must specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region in the IMS STEPLIB library field.

IMS STEPLIB library  
Specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region. Use this field if your installation stores Group options modules in separate libraries for use by ISPF and IMS. If both ISPF and IMS use the same library, this field is optional.

10. Press **F3** to save changes to the Group options.

### Refreshing CPUID options

This section describes the procedures for refreshing the CPUID options.

You can send a request to the online IMS system to refresh the CPU ID security from the standard STEPLIB/JOBLIB/link-list concatenation of your control region JCL. You do not have to restart your control region for the update to take effect.

#### To refresh the CPUID options

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).
   The Main Menu is displayed.
2. Type **4** in the selection field and press Enter.
   The Administration Menu is displayed.
3. Type **5** in the selection field and press Enter.
   The Refresh Menu is displayed.
4. Type **2** in the selection field.
5. In the **IMSID or Group** field, type an IMSID to update the CPU ID options for a single IMS system, or type a Group name to update the CPU ID options for multiple IMS systems.
   Press Enter.
   The Confirm CPU-id Refresh pop-up window is displayed.
6. Type **1** in the selection field and press Enter.
   The product refreshes the CPU ID options.
   If a Group was refreshed, the Group Refresh Results pop-up window is displayed.
Creating and formatting Log and History File data sets

This section describes the procedures for creating and formatting the Log and History File data sets.

The Log and the History File are key components of DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL. Both the Log and the History File are pairs of formatted BSAM data sets that record all product updates to a control region. Dual data sets are maintained for both the Log and the History File for recovery and reliability reasons, since both are integral to product operation. Both the dual Log data sets and the dual History File data sets must be available before any updates can be made to the control region. Only one Log data set and one History File data set is necessary for the Log and History File utilities to function.

The IMS control region must have UPDATE authority for the Log and History File data sets.

⚠️ Note

During IMS control region initialization, the IMS DB/DC SYSGEN linkedit dates are written to the Log and History File control record (if required). The Log and History File SYSGEN dates are also updated following an online change MODBLKS GEN implementation.

To create and format the Log data set

⚠️ Warning

Log format processing deletes all Log entries. After this is done, an IMS warm start (/NRE without CHKPT 0) or emergency restart (/ERE) is not possible. Therefore, you must cold start IMS after formatting the Log data sets, which will cause all restart information in the Log data sets to be lost.

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type 3 in the selection field and press Enter. The Utilities Menu is displayed.
3. Type 1 in the selection field and press Enter.
The Log Maintenance Menu is displayed.

4. Type 4 in the Log Maintenance Option selection field.

5. Type the name of the target IMSID or IMS data-sharing group in the IMSID or Group field and press Enter.

The Allocate New Log Data Set panel is displayed.

6. Enter the information for the fields that are available on the Allocate New Log Data Set panel for the primary Log data set and press Enter.

The primary Log data set is allocated.

7. Enter the information for the fields that are available on the Allocate New Log Data Set panel for the secondary Log data set and press Enter.

The secondary Log data set is allocated and the Confirm Log Format panel is displayed.

8. Type 1 in the selection field and press Enter to complete creating and formatting the Log data sets.

To create and format the History File data set

Warning

If you reformat an existing History File data set, you destroy the data set contents. You will lose all audit information concerning any changes that have been made to the control regions that are associated with the History File.

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).

The Main Menu is displayed.

2. Type 3 in the selection field and press Enter.

The Utilities Menu is displayed.

3. Type 2 in the selection field and press Enter.

The History File Maintenance Menu is displayed.

4. Type 4 in the History File Maintenance Option selection field.

5. Type the name of the target IMSID or IMS data-sharing group in the IMSID or Group field and press Enter.

The Allocate New History File Data Set panel is displayed.

6. Enter the information for the fields that are available on the Allocate New History File Data Set panel for the primary History File data set and press Enter.

The primary History File data set is allocated.

7. Enter the information for the fields that are available on the Allocate New History File Data Set panel for the secondary History File data set and press Enter.
The secondary History File data set is allocated and the Confirm History File Format panel is displayed.

8. Type 1 in the selection field and press **Enter** to complete creating and formatting the History File data sets.

**Creating View Profiles**

View Profiles allow user customization of the keyword names and descriptions used when editing DELTA Lists.

You can change the defaults for, or prohibit use of, individual fields. You can also enforce standards for DELTA Lists created at a given location or site.

If you are installing DELTA PLUS for the first time, you need to create default View Profile members. If you are using UPF security, you need to create the default View Profile members DLAKWTnn for DELTA PLUS VIRTUAL TERMINAL or DDCKWTnn for DELTA IMS for DBCTL, where nn is from the applicable UPF record. If you are using SAF security, you need to create a View Profile member named DEFAULT.

**Panel flow**

There are three ways to create a new View Profile: use the DELTA PLUS defaults, copy the values for a new View Profile from an existing View Profile, or use a conversion utility to convert existing DELTA IMS keyword tables into DELTA PLUS View Profiles.

For more information about View Profiles, see the *DELTA PLUS User Guide*.

**Using DELTA PLUS defaults**

Type the name of the new View Profile in the **View Profile** field on the View Profile Edit Entry panel and press **Enter**.

The View Profile will be populated from internal DELTA PLUS defaults.

To reset the values for the View Profile to the internal DELTA PLUS defaults, type DEFAULT on the **Command** line on the View Profile Edit panel. Press **Enter**. The View Profile will be populated from internal DELTA PLUS defaults.
Using an existing View Profile

Type the name of the new View Profile in the View Profile field on the View Profile Edit Entry panel and press Enter.

Next, type COPY name on the Command line on the View Profile Edit panel where name is the name of the existing View Profile from which you want to copy the View Profile values. Press Enter. The new values will be copied from the existing View Profile.

Using a conversion utility

DELTA PLUS provides a conversion utility to convert existing DELTA IMS keyword tables into DELTA PLUS View Profiles. Member DLP#UTL4 in the DLPCNTL data set unloaded from the DELTA PLUS product tape contains the necessary JCL for this conversion.

Instructions for using the utility are in the comments of member DLP#UTL4.

Available commands

You can issue several primary commands from the View Profile Edit, View Profile Element Edit, and View Profile Field Edit panels.

Primary commands are typed on the Command line. Uppercase characters indicate the minimum text required to execute the command.

Commands available on the View Profile Edit, View Profile Element Edit, and View Profile Field Edit panels

CANcel cancels any changes and returns to previous panel.

COPY copies data from the specified View Profile. The level of data that is copied is determined by the panel from which the COPY command is issued. For example, if you issue the COPY command from the View Profile Field Edit panel, only the data for that field type is copied.

DEFAULT populates all required fields with default values shipped with the product. The level of data that is populated is determined by the panel from which the DEFAULT command is issued. For example, if you issue the DEFAULT command from the View Profile Element Edit panel, ALL fields on the View Profile Element Edit and View Profile Field Edit panels for the selected element type will be reset to default values.

Commands available on the View Profile Edit panel

EDIT displays the View Profile Edit Entry panel to allow selection of another member for edit.

OPEN functions the same as EDIT.
**SAVe** saves the View Profile.

**Commands available on the View Profile Element Edit panel**

**ALTVIEW** toggles the current display to an alternate view. The panels in this section are all displayed in the same view. Your panel display may differ from the view of these panels. Regardless of which view you choose to display, all of the fields are still available.

**CLEAR** clears the values for the input fields on this panel for the element type you are editing.

**MACRO ON** and **MACRO OFF** toggle the current display to show IMS macro statements for the field names or to not show macro statements for the field names. The panels in this section are all displayed with **MACRO OFF**. Your panel display of a field name may differ from the view of these panels. Regardless of which view you choose to display, all of the fields are still available.

**Commands available on the View Profile Field Edit panel**

**CLEAR** clears the values for the input fields on this panel for the selected field type.

**PROMPT** displays the available values for the field on which the cursor currently resides.

**To create a View Profile**

1. From the DELTA PLUS Main Menu, type **4** in the selection field and press **Enter**. The Administration Menu is displayed.
2. Type **3** in the selection field and press **Enter**. The View Profile Edit Entry panel is displayed.
3. Type the name of the View Profile in the **View Profile** field and press **Enter**.
4. Type a **/** in the field next to each element type that you want to edit. The View Profile Element Edit panel will display for the first element type selected.

**Note**

The View Profile Element Edit panel displays different fields for the various element types. All fields displayed on any View Profile Element Edit panel are listed in the following table.

5. Edit the following fields, as necessary:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Profile</td>
<td>Displays the name of the View Profile you are creating or modifying. This is not an editable field.</td>
</tr>
<tr>
<td>Element Type</td>
<td>Displays the type of DELTA List element. Valid types are</td>
</tr>
<tr>
<td></td>
<td>• APPLCTN</td>
</tr>
<tr>
<td></td>
<td>• TRANSACT</td>
</tr>
<tr>
<td></td>
<td>• DATABASE</td>
</tr>
<tr>
<td></td>
<td>• TERMINAL</td>
</tr>
</tbody>
</table>

BMC System Administration for IMS, version 2.7.00
<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTERM</td>
<td>This is not an editable field.</td>
</tr>
<tr>
<td>RTCODE</td>
<td></td>
</tr>
<tr>
<td>SUBPOOL</td>
<td></td>
</tr>
<tr>
<td>COMMAND</td>
<td></td>
</tr>
<tr>
<td>DELTALST</td>
<td></td>
</tr>
<tr>
<td>DELTALST</td>
<td>Include another DELTA list.</td>
</tr>
</tbody>
</table>

**Description**
Type a description of the DELTA list element type. The default descriptions for each element type are:
- APPLCTN – Define program directory entry
- TRANSACT – Define transaction code
- DATABASE – Define database directory entry
- TERMINAL – Define VTAM terminal
- LTERM – Define logical terminal
- RTCODE – Define Fast Path routing code
- SUBPOOL – Define VTAM LU 6.1 SUBPOOL
- COMMAND – Execute IMS operator command
- DELTALST – Include another DELTA list

**Field Order**
Specify the Field ID number of each field in the order you want the fields to appear on the DELTA List Element Edit panel.

**Element Access**
Indicate whether to prohibit users of this View Profile access to the element type or to allow edit access.
Type 1 to allow edit access for the element type.
Type 2 to prohibit access to the element type.

**Marked for Execution**
Type a / in this field to indicate that any element of this type that is in the DELTA List should be included when the DELTA List is processed.
If this field is selected, by default, when an element of this type is added in a DELTA List it is automatically included in the execution of that DELTA List.

**Stop program before change**
Type a / in this field to indicate that the command should be executed, by default, for any element of this type when the DELTA List is processed.
If this field is selected, by default, an element of this type in a DELTA List is stopped before the change for that element is executed. For example, it is advisable on a Revise DELTA action to stop the program before executing the Revise action.

**Note**
DELTA IMS will internally issue the /DBR NOFEOV command for the DATABASE element, and /STO for all other applicable element types. If this process does not sufficiently address your requirements, additional COMMAND elements can be used.

Be aware that when performing a Fast Path database change, the /DBR command issued by DELTA IMS will take an extended amount of time if the database contains many areas. This is not an anomaly. IMS processing of the /DBR command, not DELTA IMS processing, causes the extended amount of time.

**Start program after change**
Type a / in this field to indicate that the command should be executed, by default, for any element of this type when the DELTA List is processed.
If this field is selected, by default, an element of this type in a DELTA List is /STArted after the change for that element is completed.

**Force update when queue count > 0**
This field is valid only for the TRANSACTION element type. It will not appear on the panel for the other element types.
Type a / in this field to indicate the forcing of this change, by default, for any element of this type when the DELTA List is processed.
5. If this field is selected, by default, this option allows the desired change to any element of this type in the DELTA List even if the IMS queue count is greater than zero.

**Note**

The Force option is ignored for requests that rename the transaction, revise the transaction from local to remote or vice versa, a conversational transaction where the SPA size is changed, or transactions that are changed to or from Fast Path.

Command defaults

This field is valid only for the COMMAND element type. It will not appear on the panel for the other element types. Use this field to set the default value for when an IMS command should be executed in relation to the execution of the DELTA List in which the command element is included. Type 1 to execute the command before DELTA List execution. Type 2 to execute the command after DELTA List execution.

6. Type a / in the selection field next to each element attribute for which you want to edit the default values. The View Profile Field Edit panel will display for the first element attribute field selected.

**Note**

The View Profile Field Edit panel displays different fields depending upon which element attribute field was selected for editing. All fields displayed on any View Profile Field Edit panel are listed in the following table.

7. Edit the following fields, as necessary:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Profile</td>
<td>Displays the name of the View Profile you are creating or modifying. This is not an editable field.</td>
</tr>
</tbody>
</table>
| Element Type | Displays the type of DELTA List element. Valid types are:  
  - APPLCTN  
  - TRANSACT  
  - DATABASE  
  - TERMINAL  
  - LTERM  
  - RTCODE  
  - SUBPOOL  
  - COMMAND  
  - DELTALST  
  This is not an editable field. |
| Field ID | The Field ID is a sequential ID number of each element attribute field that appears for the element type on the DELTA List Element Edit panel. This is not an editable field. |
| Field Name | Displays the name of the element attribute field you are modifying. This is not an editable field. |
### Field name | Description
--- | ---
Macro | Specify the corresponding IMS macro statement for this element attribute field.
Description | Type a user-defined description of this element attribute field.
Field access | Indicate whether to prohibit users of this View Profile access to this element attribute field, or to allow read-only or edit access. Type 1 to allow edit access for this field. Type 2 to allow read-only access for this field. Type 3 to prohibit access to this field.
Default value | This field is not applicable to all element attribute fields. Specify a default value for the element attribute field.
Select field for revise | This field is not applicable to all element attribute fields. Type a / in this field to indicate that this element attribute field should be selected for revise when an element of this type is added to a DELTA List with a DELTA action of REVISE. If this field is selected, by default, this element attribute field will be selected for revise when an element of this type is added with a DELTA action of REVISE.
Comment | This field is applicable only to the comment element attribute fields. Use this field to provide any miscellaneous comments about this element type or any of the element attribute fields.
Remarks | Type any miscellaneous comments about this element attribute field.


| Previous action | Result |
--- | ---
You selected more than one element attribute field for editing. | The View Profile Field Edit panel is displayed for the next field. Repeat step 7 (see page 94) and step 8 (see page 95) until the View Profile Element Edit panel is displayed for the element type selected for editing. Go to step 9 (see page 95). |
You selected only one element attribute field for editing. | The View Profile Element Edit panel is displayed for the element type selected for editing. Go to step 10 (see page 95). |


| Previous action | Result |
--- | ---
You selected more than one element type for editing. | The View Profile Element Edit panel is displayed for the next element type. Repeat steps step 5 through 8 (see page 92) until the View Profile Edit panel is displayed. Go to step 10 (see page 95). |
You selected only one element type for editing. | The View Profile Edit panel is displayed. Go to step 10 (see page 95). |

#### 10. Save your changes.

a. Press F3. The Confirm View Profile Save pop-up window is displayed.
b. Type 1 in the selection field and press Enter. DELTA PLUS saves the View Profile.
c. Press F3 twice (or three times if you are on the member selection list panel). The DELTA PLUS Main Menu is displayed.
Editing View Profiles

This section describes the procedures for editing View Profiles.

View Profiles allow you to customize the keyword names and descriptions that are used to edit DELTA Lists. You can change the defaults for or prohibit use of individual fields. You can also enforce standards for DELTA Lists that are created at a given location or site.

You can issue several primary commands from the View Profile Edit, View Profile Element Edit, and View Profile Field Edit panels. Type primary commands on the Command line. Uppercase characters indicate the minimum text that is required to execute the command.

The following table lists the commands and the panels from which you can issue them, and provides a description of each command.

### Commands available when editing View Profiles

<table>
<thead>
<tr>
<th>Command</th>
<th>Can be issued from panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CANcel</td>
<td>View Profile Edit</td>
<td>Cancels any changes and returns to the previous panel</td>
</tr>
<tr>
<td>COPY</td>
<td>View Profile Element Edit, View Profile Field Edit</td>
<td>Copies data from the specified View Profile. The panel from which the command is issued determines the level of data that is copied. For example, if you issue the command from the View Profile Field Edit panel, only the data for that field type is copied.</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>View Profile Element Edit, View Profile Field Edit</td>
<td>Populates all required fields with default values that are shipped with the product. The panel from which the command is issued determines the level of data that is populated. For example, if you issue the command from the View Profile Element Edit panel, ALL fields on the View Profile Element Edit and View Profile Field Edit panels for the selected element type will be reset to default values.</td>
</tr>
<tr>
<td>EDIT</td>
<td>View Profile Edit</td>
<td>Displays the View Profile Edit Entry panel to allow selection of another member for edit</td>
</tr>
<tr>
<td>OPEN</td>
<td>View Profile Edit</td>
<td>Performs the same function as EDIT</td>
</tr>
<tr>
<td>SAVE</td>
<td>View Profile Edit</td>
<td>Saves the View Profile</td>
</tr>
<tr>
<td>ALTVIEW</td>
<td>View Profile Element Edit</td>
<td>Toggles the current display to an alternate view</td>
</tr>
<tr>
<td>CLEAR</td>
<td>View Profile Element Edit</td>
<td>Clears the values for the input fields for the element type that you are editing</td>
</tr>
<tr>
<td>MACRO ON</td>
<td>View Profile Element Edit</td>
<td>Toggles the current display to show or not show IMS macro statements for the field names</td>
</tr>
<tr>
<td>MACRO OFF</td>
<td>View Profile Element Edit</td>
<td></td>
</tr>
<tr>
<td>CLEAR</td>
<td>View Profile Field Edit</td>
<td>Clears the values for the input fields for the selected field type</td>
</tr>
<tr>
<td>PROMPT</td>
<td>View Profile Field Edit</td>
<td>Displays the available values for the field on which the cursor currently resides</td>
</tr>
</tbody>
</table>
To edit a View Profile

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.

2. From the Main Menu, type 4 in the selection field and press Enter. The Administration Menu is displayed.

3. Type 3 in the selection field and press Enter. The View Profile Edit Entry panel is displayed.

   **View Profile Edit Entry panel**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELTA PLUS</td>
<td>View Profile Edit Entry</td>
<td></td>
</tr>
<tr>
<td>Command ===&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Specify the View Profile you wish to edit.
   View Profile . . . . . . . _______ (blank for selection list)

4. Perform the appropriate action and press Enter.

   **Activity** | **Action**
   ---------------|-------------------
   Indicate a specific View Profile that you want to edit or create. | Type the name of the View Profile in the View Profile field.

   Choose a View Profile that you want to edit from a list of View Profiles. | Leave the View Profile field blank.

   The next panel is displayed based on the action that you performed.

   **Previous action** | **Result**
   -------------------|-------------------
   You typed a specific View Profile name in the View Profile field. | The View Profile Edit panel is displayed. Go to Step 6 (see page 98).
   You left the View Profile field blank. | A Member Selection List panel is displayed, allowing you to select a View Profile. Go to Step 5 (see page 98).

   **Member Selection List panel**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Functions</th>
<th>Utilities</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDIT</td>
<td>DLP.VPROFILE.LIB</td>
<td>Row 00001 of 00002</td>
<td></td>
</tr>
<tr>
<td>Command ===&gt;</td>
<td></td>
<td>Scroll ===&gt; PAGE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Prompt</th>
<th>Size</th>
<th>Created</th>
<th>Changed</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td></td>
<td>174</td>
<td>1999/02/15</td>
<td>1999/05/11 10:55:15</td>
<td>RIHWXC2</td>
</tr>
<tr>
<td>DBCTL2</td>
<td></td>
<td>172</td>
<td>1999/10/19</td>
<td>1999/10/19 13:35:26</td>
<td>RIHWXC2</td>
</tr>
</tbody>
</table>

   **End**
5. Type **S** next to the View Profile that you want to edit and press **Enter**. The View Profile Edit panel is displayed.

**View Profile Edit panel**

```
<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
</table>
```

DELTA PLUS

View Profile . : DEFAULT

Enter '//' below to edit the View Profiles for the listed element types.

<table>
<thead>
<tr>
<th>Element</th>
<th>Type</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLCTN</td>
<td>Define program directory entry</td>
<td>EDIT</td>
<td></td>
</tr>
<tr>
<td>TRANSACT</td>
<td>Define transaction Code</td>
<td>EDIT</td>
<td></td>
</tr>
<tr>
<td>DATABASE</td>
<td>Define data base directory entry</td>
<td>EDIT</td>
<td></td>
</tr>
</tbody>
</table>

6. Type **/** in the field next to each element type that you want to edit.

The View Profile Element Edit panel for the first element type that you selected is displayed.

**View Profile Element Edit panel**

```
<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>View</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
</table>
```

DELTA PLUS

View Profile . : DEFAULT

Element Type . : APPLCTN

Description . : Define Program directory entry


Element Access.
1. Edit
   / Marked for execution
2. None
   / Stop program before change
   / Start program after change

Fields. Enter '//' to edit the View Profiles for the listed fields.

<table>
<thead>
<tr>
<th>ID Field</th>
<th>Description</th>
<th>Value Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PSB=</td>
<td>Name of application ..................</td>
<td>EDIT</td>
</tr>
<tr>
<td>2 Rename</td>
<td>New name (valid for REV only) ...</td>
<td>EDIT</td>
</tr>
<tr>
<td>3 Model after</td>
<td>Model after (valid for ADD,REV,ADDREV).</td>
<td>EDIT</td>
</tr>
<tr>
<td>4 RESIDENT=</td>
<td>PSB resident in storage?...</td>
<td>NO EDIT</td>
</tr>
<tr>
<td>5 PGMTYPE=</td>
<td>Program is an MPP or BMP. ...</td>
<td>TP EDIT</td>
</tr>
<tr>
<td>6 SHTNDTP=</td>
<td>Schedule serial or parallel .......</td>
<td>SERIAL EDIT</td>
</tr>
<tr>
<td>7 FTPATH=</td>
<td>Fast Path program? ..................</td>
<td>NO EDIT</td>
</tr>
</tbody>
</table>

⚠️ **Note**
The View Profile Element Edit panel displays different fields for the COMMAND and TRANSACT element types than those that are shown in previous figure. The View Profile Element Edit panel for the DELTALST element type only displays some of the fields that are shown in the previous figure.

The following fields are available on this panel:

**View Profile**

The name of the View Profile that you are creating or modifying. This is not an editable field.

**Element Type**

Displays the type of DELTA List element. Valid types are:

- APPLCTN
- TRANSACT
- DATABASE
- TERMINAL
- LTERM
- RTCODE
- SUBPOOL
- COMMAND
- DELTALST

This is not an editable field.

**Description**

A description of the DELTA List element type. The default descriptions are:

- APPLCTN-Define program directory entry
- TRANSACT-Define transaction code
- DATABASE-Define database directory entry
- TERMINAL-Define VTAM terminal
- LTERM-Define logical terminal
- RTCODE-Define Fast Path routing code
- SUBPOOL-Define VTAM LU 6.1 SUBPOOL
- COMMAND-Execute IMS operator command
- DELTALST-Include another DELTA List

**Field Order**

The field ID number of each field in the order in which you want the fields to appear on the DELTA List Element Edit panel.

**Element Access**

Indicates whether to prohibit users of this View Profile from accessing the element type or to allow edit access.

- 1 allows edit access for the element type.
- 2 prohibits access to the element type.

**Marked for Execution**

A / in the selection field includes any element of this type that is in the DELTA List when the DELTA List is processed.

If you select this field, by default, when you add an element of this type to a DELTA List, it is automatically included in the DELTA List execution.

**Stop program before change**

A / in the selection field indicates that the command should be executed, by default, for any element of this type when the DELTA List is processed.
If you select this field, by default, an element of this type in a DELTA List is stopped before the change for that element is executed. For example, it is advisable on a Revise DELTA action to stop the program before executing the Revise action.

**Note**

The product will internally issue the `/DBR NOFEOV` command for the DATABASE element, and `/STO` for all other applicable element types. If this process does not sufficiently address your requirements, you can use additional COMMAND elements.

Be aware that when performing a FAST PATH database change, the `/DBR` command that DELTA IMS issues will take an extended amount of time if the database contains many areas. This is not an anomaly. IMS processing of the `/DBR` command, not DELTA IMS processing, causes the extended amount of time.

**Start program after change**

A `/` in the selection field indicates that the command should be executed, by default, for any element of this type when the DELTA List is processed.

If you select this field, by default, an element of this type in a DELTA List is `/STARTed after the change for that element is completed. Force update when queue count > 0`

**Note**

This field is valid only for the TRANSACTION element type. It will not appear on the panel for the other element types.

A `/` in the selection field indicates that the change will be forced, by default, for any element of this type when the DELTA List is processed.

By default, selecting this field allows the desired change to any element of this type in the DELTA List, even if the IMS queue count is greater than zero.

**Note**

The Force option is ignored for requests that rename the transaction, requests that revise the transaction from local to remote or vice versa, a conversational transaction where the SPA size is changed, or transactions that are changed to or from FAST PATH.

**Command defaults**

**Note**
This field is valid only for the **COMMAND** element type. It will not appear on the panel for the other element types.

Sets the default value for when an IMS command should execute in relation to the execution of the DELTA List in which the command element is included.

1. **1** executes the command before DELTA List execution.
2. **2** executes the command after DELTA List execution.

7. **Type a /** in the selection field next to each element attribute for which you want to edit the default values.

The View Profile Field Edit panel for the first element attribute field that you selected is displayed.

**View Profile Field Edit panel**

```
File  Edit  Options  Help
-------------------------------------------------------------------------------
DELTA PLUS                    View Profile Field Edit

View Profile       : DEFAULT
Element Type       : APPLCTN
Field ID . . . : 01    Field Name: PSB=
Macro . . . . . PSB= . . . . . . . . . . . . . . . . . .
Description . . Name of application . . . . . . . . . .

Field access.
  1  Edit
  2  Read only
  3  None

Remarks . . . __________
```

**Note**

The View Profile Field Edit panel displays different fields than those that are displayed in the previous figure, depending upon which element attribute field was selected for editing.

The following fields are available on this panel:

**View Profile**
The name of the View Profile that you are creating or modifying. This is not an editable field.

**Element Type**
Displays the type of DELTA List element. Valid types are:

- **APPLCTN**
- **TRANSACT**
- **DATABASE**
- TERMINAL
- LTERM
- RTCODE
- SUBPOOL
- COMMAND
- DELTALST

This is not an editable field.

**Field ID**
A sequential number for each element attribute field that appears for the element type on the DELTA List Element Edit panel. This is not an editable field.

**Field Name**
The name of the element attribute field that you are modifying. This is not an editable field.

**Macro**
The IMS macro statement that corresponds to this element attribute field.

**Description**
A user-defined description for this element attribute field.

**Field access**
Indicates whether to prohibit users of this View Profile from accessing this element attribute field or to allow read-only or edit access.

1 allows edit access for this field.
2 allows read-only access for this field.
3 prohibits access to this field.

**Default value**

**Note**
This field is not applicable to all element attribute fields.

The default value for the element attribute field. **Select field for revise**

**Note**
This field is not applicable to all element attribute fields.

A / in the selection field indicates that this element attribute field should be selected for revise when an element of this type is added to a DELTA List with a DELTA action of REVISE.

If you select this field, by default, this element attribute field will be selected for revise when an element of this type is added with a DELTA action of REVISE. **Comment**
Note

This field applies only to the comment element attribute fields.

Comments about this element type or any of the element attribute fields.

Remarks

Comments about this element attribute field.

8. Edit the desired fields and press F3.

The next panel is displayed based on your previous action.

<table>
<thead>
<tr>
<th>Previous action</th>
<th>Result</th>
<th>Action to take</th>
</tr>
</thead>
</table>
| You selected more than one element attribute field for editing. | The View Profile Field Edit panel (Figure 5 (see page 101)) is displayed for the next field. | a. Repeat Step 8 (see page 103) until the View Profile Element Edit panel (Figure 4 (see page 98)) is displayed for the element type that you selected for editing.  
  b. Go to Step 9 (see page 103). |
| You selected only one element attribute field for editing.     | The View Profile Element Edit panel (Figure 4 (see page 98)) is displayed for the element type that you selected for editing. | Go to Step 9 (see page 103). |


The next panel is displayed based on your previous action.

<table>
<thead>
<tr>
<th>Previous action</th>
<th>Result</th>
<th>Action to take</th>
</tr>
</thead>
</table>
| You selected more than one element type for editing. | The View Profile Element Edit panel (Figure 4 (see page 98)) is displayed for the next element type. | a. Repeat Step 7 (see page 101) and Step 8 (see page 103) until the View Profile Edit panel (Figure 3 (see page 98)) is displayed.  
  b. Go to Step 10 (see page 103). |
| You selected only one element type for editing.     | The View Profile Edit panel (Figure 3 (see page 98)) is displayed.     | Go to Step 10 (see page 103). |

10. Press F3 to save your changes.

To create a new View Profile

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).

   The Main Menu is displayed.

2. Type 4 in the selection field and press Enter.

   The Administration Menu is displayed.

3. Type 3 in the selection field and press Enter.

   The View Profile Edit Entry panel is displayed.

4. Determine the method that you want to use to create the new View Profile:
<table>
<thead>
<tr>
<th>If you want to create the new View Profile by</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the product defaults</td>
<td>Step 5 (see page 104)</td>
</tr>
<tr>
<td>Copying options from an existing View Profile</td>
<td>Step 6 (see page 104)</td>
</tr>
</tbody>
</table>

5. Type the name of the new View Profile in the View Profile field and press **Enter**. Internal product defaults will populate the View Profile.

6. Type the name of the new View Profile in the View Profile field and press **Enter**. The View Profile Edit panel is displayed.

7. Type **COPY name** on the Command line (where name is the name of the existing View Profile from which you want to copy the new View Profile values) and press **Enter**. The new values are copied from the existing View Profile.

⚠️ **Note**

To reset the values for the View Profile to the internal product defaults, type **DEFAULT** on the Command line on the View Profile Edit panel and press Enter. Internal product defaults will populate the View Profile.

## Allocating new data sets

This section describes the steps for allocating new data sets.

You can allocate the following data sets:

- Log
- History File
- DELTA List library
- options library
- View Profile library
- Variable Definition library
- Report output data sets
- User access profiles data sets
- Repository data sets

### To allocate a new data set

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type **4** in the selection field and press **Enter**.  
The Administration Menu is displayed.

3. Type **7** in the selection field and press **Enter**.  
The Data Set Allocation Menu is displayed.

**Data Set Allocation Menu**

<table>
<thead>
<tr>
<th>Menu Options Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELTA PLUS VT Data Set Allocation Menu</td>
</tr>
<tr>
<td>Command ===&gt; ________________________________</td>
</tr>
</tbody>
</table>

Choose the type of data set to allocate.

1. DELTA List library - Contains DELTA Lists
2. Options library - Contains IMSID and Group Options
3. View Profile library - Contains Edit View Profiles
4. Variable Definition library - Contains Variable Definition Sets
5. Log data set - Primary or Secondary Log data set
6. History file data set - Primary or Secondary History File data set
7. Report output data set - Output data set for reports or conversions
8. User Access Profiles (UPF) - Contains internal security profiles
9. Repository data set - Primary or Secondary Repository data set

Specify the data set to allocate.

Data set name . . . ________________________________

4. Type the number that corresponds to the type of data set that you want to create in the selection field.

5. Type the name of the data set to be allocated in the **Data set name** field and press **Enter**.  
The Allocate New **data_set_type** panel is displayed.

**Allocate New Variable Definition Library panel**

<table>
<thead>
<tr>
<th>Menu Options Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocate New Variable Definition Library</td>
</tr>
<tr>
<td>Command ===&gt; ________________________________</td>
</tr>
</tbody>
</table>

Enter information below to allocate the data set. Then press Enter.

Variable Definition library: 'DLP.VARDEF.LIB'

Enter allocation information:

- SMS Management class . . . ________ (For SMS managed data set)
- SMS Storage class . . . ________ (For SMS managed data set)
- Volume serial . . . . . . ________
- Generic unit . . . . . . ________
- Space units . . . . . . ________ (TRKS or CYLS)
- Primary quantity . . . . . . ________ (in above units)
- Secondary quantity . . . . . . ________ (in above units)
- Directory blocks . . . . . . ________
The panels that you can access from the Data Set Allocation Menu will be named Allocate New data_set_type, where data_set_type is:

- DELTA List Library
- Options Library
- View Profile Library
- Variable Definition Library
- Log Data Set
- History File Data Set
- Report Output Data Set
- UPF Data Set
- Repository data set

⚠️ Note

The IMS control region must have UPDATE authority for the Log and History File data sets.
During IMS control region initialization, the IMS DB/DC SYSGEN linkedit dates are written to the Log and History File control record (if required). The Log and History File SYSGEN dates are also updated following an online change MODBLKS GEN implementation.

The following fields are possible for these panels: data_set_type
The type of data set that you are allocating. This is not an editable field.

SMS Management class
The SMS management class to be used for the data set allocation. This field is not required unless your installation requires the use of SMS.

SMS Storage class
The SMS storage class to be used for the data set allocation. This field is not required unless your installation requires the use of SMS.

Volume serial
The DASD volume serial (VOLSER) where the data set will be allocated.

Generic unit
The generic unit name to be used for the data set allocation. Generic names (also referred to as esoteric) are given to groups, or pools, of DASD volumes. Some common generic/esoteric names are SYSDA, SYSALLDA, and SCRATCH.

Space units
The space unit type to be used for the data set allocation. Valid values are TRKS or CYLS.

Primary quantity
The number of primary space units to be used for the data set allocation. You previously specified the space unit type on this panel.

Secondary quantity
The number of secondary space units to be used for the data set allocation. You previously specified the space unit type on this panel.

Directory blocks
The number of directory blocks to be provided for a partitioned data set. Specify zero for a sequential data set. **Block size**
The DASD block size to be used for the data set.

6. Edit the fields as necessary and press **Enter**.
The Data Set Allocation Menu is displayed and the data set is allocated.

## Adding an IMSID to an existing Group's Log data sets

This section describes the procedures for adding an IMSID to an existing Group’s Log data sets.

The Add IMSID to Group Log option allows you to add an IMSID to the Log and History File data sets for a specified Group. This feature ensures that the coordinated changes that have already been applied to the IMSIDs in the specified Group will also be applied to the IMSID that you are adding to the Group.

### To add an IMSID to an existing Group’s Log data sets

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in _Accessing the products from an ISPF options menu_ (see page 57) or through the CLIST that you created in _Accessing the products from a CLIST_ (see page 57). The Main Menu is displayed.
2. Type **4** in the selection field and press **Enter**.
The Administration Menu is displayed.
3. Type **2** in the selection field and press **Enter**.
The IMSID/Group Options Entry panel is displayed.
4. Type the IMSID to be added in the **IMSID or Group** field, type **1** in the selection field, and press **Enter**.
The Edit IMSID Options panel for your product is displayed.
5. (_DELTA PLUS VIRTUAL TERMINAL only_) Type **1** in the selection field and press **Enter**.
The IMSID Options – Basic Options panel is displayed.
6. Type the name of the Group to which you want to add an IMSID in the **XCF Group** field and press **Enter**.
The Confirm Add IMS pop-up window is displayed.

**Confirm Add IMS Pop-up window**

```
<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>Refresh</th>
<th>Format</th>
<th>AddIMS</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ===&gt;</td>
<td>Confirm Add IMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you want to add IMSA to the Log and History File data sets for Group GRPJ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
6. Adding the IMSID to the Group Log will allow all active coordinated changes for the Group to be applied to IMSA when it is started.
   Choose one selection.
   1. Yes, add the IMSID to the Log and History File.
   2. No, cancel adding the IMSID.
   CAUTION: Adding an IMSID will temporarily destroy both DELTA PLUS Log data sets. During this time period, an IMS restart will not be possible.
   Ensure that you have a current backup of the Log data sets before continuing.

7. Type 1 in the selection field to add the IMSID to the specified Group’s Log and History File data sets.

Note

If you type 2 in the selection field, the IMSID is not added to the specified Group’s Log and History File data sets, but the change to the XCF Group field that you made in Step 6 (see page 107) is saved to the options for the IMSID when you save your changes.
You can add the IMSID to the specified Group’s Log and History File data sets later.

8. Press F3 to save the changes.

To add the IMSID to the specified Group’s Log and History File data sets later

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).

   The Main Menu is displayed.

2. Type 4 in the selection field and press Enter.

   The Administration Menu is displayed.

3. Type 8 in the selection field and press Enter.

   The Add IMSID to Group Log panel is displayed.

   Add IMSID to Group Log panel
4. In the **Add IMSID** field, type the IMSID of the IMS system that you want to add to a specified Group's Log and History File data sets.

5. In the **to the Log for Group** field, type the name of the Group for which you want to add an IMSID to the Log and History File data sets and press **Enter**.
   The Confirm Add IMS pop-up window is displayed.

6. Type 1 in the selection field and press **Enter**.
   The IMSID is added to the specified Group's Log and History File data sets.

---

**Completing DELTA PLUS VIRTUAL TERMINAL customization**

The customization tasks that are described in this section apply to DELTA PLUS VIRTUAL TERMINAL only.

**Enabling DELTA PLUS VIRTUAL TERMINAL**

DELTA PLUS VIRTUAL TERMINAL
Before you complete the customization tasks for DELTA PLUS VIRTUAL TERMINAL, you should ensure that it is enabled.

To enable DELTA PLUS VIRTUAL TERMINAL, select the **Enable DELTA PLUS VIRTUAL TERMINAL** option on the IMSID Options - VT Options panel.

DELTA PLUS VIRTUAL TERMINAL

To use DELTA PLUS VIRTUAL TERMINAL, you must also disable ETO. To disable ETO, you can perform either of the following actions:

- Exclude ETO from the IMSGEN
- Include ETO in the IMSGEN, but specify ETO=N or ETO=M in member DFSPB_yyy of your IMS PROCLIB

**Setting virtual terminal IMSID options**

This section describes procedures for setting virtual terminal IMSID options.
To completely configure the IMSID options module for DELTA PLUS VIRTUAL TERMINAL, you must also set basic IMSID options. For more information, see Setting IMSID options when installing DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL. (see page 75).

To set virtual terminal IMSID options, perform the following steps:

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57). The Main Menu is displayed.
2. Type 4 in the selection field and press Enter. The Administration Menu is displayed.
3. Type 2 in the selection field and press Enter. The IMSID/Group Options Entry panel is displayed.

**IMSID/Group Options Entry panel**

4. Type 1 in the selection field.
5. Type the data set name of the library in which the VIRTUAL TERMINAL IMSID options module (DLA#, where # is the IMSID) resides in the Options library field. For information about allocating the options library, see Allocating new data sets (see page 104).
6. Perform the appropriate action.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicate a specific IMSID for the IMS system that you want to customize or access.</td>
<td>Type the IMSID of the IMS system in the <strong>IMSID or Group</strong> field.</td>
</tr>
<tr>
<td>Choose an IMSID that you want to customize or access from a list of IMSIDs.</td>
<td>Leave the <strong>IMSID or Group</strong> field blank.</td>
</tr>
</tbody>
</table>
7. *(optional)* If your installation stores DELTA PLUS VIRTUAL TERMINAL IMSID/Group options modules in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the IMSID options modules in the *Save library* field. If ISPF, IMS, and BMCXLINK use the same library, this field is optional.

**Note**

If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

Press **Enter**.

If you typed a specific IMSID in the IMSID or Group field, the Edit IMSID Options panel is displayed. Go to **Step 9 (see page 112)**.

If you left the IMSID or Group field blank, the Edit IMSID Options – List panel is displayed, allowing you to select an IMSID. Go to **Step 8 (see page 111)**.

**Edit IMSID Options - List panel**

<table>
<thead>
<tr>
<th>Options Library . . : 'ABC.DLP.OPTIONS.LOAD'</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter <strong>S</strong> to edit the IMSID options.</td>
</tr>
<tr>
<td>_ _ ABCD</td>
</tr>
<tr>
<td>_ _ BAD1</td>
</tr>
<tr>
<td>_ _ GCB5</td>
</tr>
<tr>
<td>_ _ MJD5</td>
</tr>
<tr>
<td>_ _ NEW</td>
</tr>
<tr>
<td>_ _ PXMI</td>
</tr>
<tr>
<td>_ _ TEST</td>
</tr>
<tr>
<td>_ _ WXCA</td>
</tr>
<tr>
<td>_ _ WXCB</td>
</tr>
<tr>
<td>_ _ WXCC</td>
</tr>
<tr>
<td>_ _ WXCD</td>
</tr>
<tr>
<td>_ _ WXCG</td>
</tr>
<tr>
<td>_ _ WXCK</td>
</tr>
<tr>
<td>_ _ WXCD</td>
</tr>
<tr>
<td>_ _ WXCR</td>
</tr>
<tr>
<td>_ _ WXCT</td>
</tr>
</tbody>
</table>

8. Type **S** next to the IMSID you want to customize or access and press **Enter**.

The Edit IMSID Options panel is displayed.

**Edit IMSID Options panel**
8. Continue to the appropriate section based on the options that you want to set.

<table>
<thead>
<tr>
<th>If you want to set</th>
<th>Continue to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limits for virtual terminals</td>
<td>Setting limits for virtual terminals (see page 112)</td>
</tr>
<tr>
<td>Virtual terminal options</td>
<td>Setting virtual terminal options (see page 114)</td>
</tr>
<tr>
<td>Virtual terminal TSS options</td>
<td>Setting virtual terminal TSS options (see page 116)</td>
</tr>
<tr>
<td>Virtual terminal logon options</td>
<td>Setting virtual terminal logon options (see page 117)</td>
</tr>
<tr>
<td>Virtual terminal signon bypass options</td>
<td>Setting virtual terminal signon bypass options (see page 119)</td>
</tr>
<tr>
<td>Virtual terminal signon options</td>
<td>Setting virtual terminal logon options (see page 117)</td>
</tr>
<tr>
<td>Extended options</td>
<td>Setting extended options (see page 122)</td>
</tr>
</tbody>
</table>

**Setting limits for virtual terminals**

This section describes the steps for setting virtual terminal limits for a specific IMS.

1. From the Edit IMSID Options panel, type 2 in the selection field and press **Enter**.

   The IMSID Options – VT Limits panel is displayed.

   The following fields are available on this panel:

   **IMSID**

   The IMSID of the options module that you selected. This is not an editable field.

   **Maximum /SECURE ALLOWed users**

   The maximum number of user IDs that can be specified by a /SECURE ALLOW command between IMS cold starts.

   DELTA PLUS VIRTUAL TERMINAL uses this value to calculate the size and capacity of the userid pool, VTFUSBPL, which is allocated in the IMS private area during initialization. This value is optional; 0 indicates that no userid pool is allocated.
If this value is too low, it can cause /SECURE ALLOW commands to fail. If this value is too high, it can waste private area virtual storage, but it will not create more overhead.
The initial value is site-dependent. Although you may increase the value without impacting IMS operation, it will not take effect until the next IMS restart. A cold start is recommended if you decrease the value.

**Maximum virtual printer overrides**
The maximum number of virtual printer overrides in effect at the same time that can be specified by an /ASSIGN command.
DELTA PLUS VIRTUAL TERMINAL uses this value to calculate the size and capacity of the VPO pool, VTFVPOPL, which is allocated in the IMS private area during initialization. This value is optional; 0 indicates that no VPO pool is allocated.
If this value is too low, it can cause /ASSIGN commands for virtual printers to fail. If this value is too high, it can waste private area virtual storage, but it will not create more overhead.
The initial value is site-dependent. Although you can increase the value without impacting IMS operation, it will not take effect until the next IMS restart. A cold start is recommended if you decrease the value.

**Maximum virtual terminal pending entries**
The maximum number of virtual terminal pending entries that can be in effect at the same time.
This value is ignored when Resource Manager (RM) and IMSPLEX Terminal Management are in use.
DELTA PLUS VIRTUAL TERMINAL uses this value to calculate the size and capacity of the VTE pool, VTFVTEPL, which is allocated in the IMS private area during initialization. 0 indicates that no VTE pool is allocated.
If this value is too low, it can cause virtual terminal /EXCL, /STOP, /TRA, or /TEST MFS commands to fail. If this value is too high, it can waste private area virtual storage, but it will not create more overhead.
You can change the value without impacting IMS operation, but it will not take effect until the next IMS restart. A cold start is recommended if you decrease the value.

**Tip**
You should specify a non-zero number for both VPOs and VTEs. If you specify a non-zero value, you will be able to specify a virtual printer override and set nodes in test MFS in emergency situations. BMC recommends that you specify a value of at least 10 for both VPOs and VTEs.

**Idle terminal logoff intervals**
The number of minutes a virtual terminal can remain inactive before an automatic logoff is invoked. The logon/signon process can select the alternate interval. For more information about automatic logoff, see the *DELTA PLUS User Guide*. 
A valid terminal logoff interval is 0 or a value between 10 and 999 minutes.

**Idle conversation logoff intervals**
The number of minutes a virtual terminal in conversational mode can remain inactive before an automatic logoff is invoked. This value overrides the idle terminal logoff interval specified in the previous field if the terminal is in conversational mode. When a virtual terminal is logged off, conversations are assigned to the user/SPQB that was created when the terminal was logged on. The conversations remain in the state they were in when the terminal was logged off. This option only logs off the terminal; it does not exit the conversations.

The logon/signon process can select the alternate interval. For more information about automatic logoff, see the *DELTA PLUS User Guide.*

A valid logoff interval for a terminal in conversation is 0 or a value between 10 and 999 minutes.

**Idle virtual printer logoff intervals**
The number of minutes a virtual printer can remain inactive before an automatic logoff is invoked. You can specify use of the alternate interval via the virtual printer timer override. For information about creating TSS tables, see the *DELTA PLUS User Guide.* The alternate value, entered in minutes, specifies how long a virtual printer may remain inactive before an automatic logoff will be invoked.

Virtual printers that use models defined to IMS with OPTIONS=DISCON are automatically logged off when the queue count is zero. The OPTIONS=DISCON parameter takes precedence over any value that you specify in this field. This option also takes precedence over the No Automatic Timeout option in a Virtual Printer Timer Override table.

**Held conversation exit interval**
This field is optional. The number of minutes a virtual terminal waits before exiting a held conversation, whether the conversation was initiated and held on a virtual terminal or an IMSGEN-defined terminal. 0 indicates that no held conversations are to be exited. Held conversations can be exited only if the terminal is stopped or disconnected. This interval is independent of the idle conversation logoff intervals; it does not begin after the expiration of the idle conversation logoff interval. For example, if a held conversation exceeds the held conversation exit interval while still assigned to an active terminal, the conversation will be immediately exited when the terminal logs off or is automatically logged off due to inactivity.

2. Edit the fields as necessary.
3. Save the changes to the virtual terminal limits.

---

**Setting virtual terminal options**

This section describes the steps for setting virtual terminal options for a specific IMS.

1. From the Edit IMSID Options panel, type 3 in the selection field and press **Enter**.
The IMSID Options – VT Options panel is displayed.
The following fields are available on this panel:
<table>
<thead>
<tr>
<th><strong>IMSID</strong></th>
<th>The IMSID of the options module that you selected. This is not an editable field.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable DELTA PLUS VIRTUAL TERMINAL</strong></td>
<td>A / indicates to activate DELTA PLUS VIRTUAL TERMINAL.</td>
</tr>
<tr>
<td><strong>Notify MTO of auto logoffs and exits</strong></td>
<td>A / indicates to send a message to the IMS Master Terminal each time DELTA PLUS VIRTUAL TERMINAL automatically logs off an idle virtual terminal or automatically exits a conversation.</td>
</tr>
<tr>
<td><strong>Require signon for ALL virtual terminals</strong></td>
<td>A / indicates that a signon is required after a virtual terminal logon. A signon is required for DELTA PLUS VIRTUAL TERMINAL enhanced conversation and message-handling features to associate conversations and messages with a userid.</td>
</tr>
</tbody>
</table>

**Note**
If any users are not required to sign on, do not specify signon required. All users will attempt signon bypass if you do not specify signon required. If signon bypass is not successful, the user will still be required to sign on.

**Support multiple concurrent LTERMs for virtual terminals**
A / enables multiple concurrent LTERM support for virtual terminals. If you select this option, each virtual terminal can support up to eight LTERM names. The node and LTERMS must be virtual. When you do not want multiple LTERMs, the argument length in the Translate Subsystem Services (TSS) table for Signon Bypass options 2 and 3 and Signon options 3 and 4 must equal eight; otherwise, the argument length must be greater than eight to permit suffixed node or userid values.

**Warning**
Using a multiple LTERM per node TSS table for signon or signon bypass requires a special TSS translation, which precludes the use of pattern masking in these tables.

**Tip**
Use this option only if your NTERM table has at least one node with more than one LTERM. This does not pertain to using a node as the LTERM and signing on multiple times.

<table>
<thead>
<tr>
<th><strong>VT system log code</strong></th>
<th>The log code that DELTA PLUS VIRTUAL TERMINAL will use when it writes records to the IMS system log. Use any hexadecimal number from X'00' to X'7F', except X'DA'. The default is X'DE'.</th>
</tr>
</thead>
</table>
| **DFS3649A /SIGN COMMAND REQUIRED format name** | The name of a Message Output Descriptor (MOD) that displays each time logon occurs at a VTAM terminal where signon is required. The following MODs may be used in this field:  
  • user-customized MOD
    The user's own MOD may be used; however, it should contain a SYSMSG field.  
  • IBM default MOD
    The IBM default MOD DFS3649A /SIGN COMMAND REQUIRED is displayed if the field is left blank. If a signon failure occurs, a message describing the failure will be displayed in the SYSMSG field of the MOD used. To change the message text, use sample JCL in DLPCNTL member DLA#SMSG to assemble and link a replacement module called VTFSMSG0. |

---

BMC System Administration for IMS, version 2.7.00

Page 115 of 284
1. **DFS3650I SESSION STATUS format name**

   The name of a Message Output Descriptor (MOD) that displays each time a VTAM terminal which is not required to sign on, logs on to IMS.

   - If a MOD name has not been supplied and the terminal logs on, the IBM default message DFS3650I SESSION STATUS is displayed.
   - If a MOD name has been supplied and the terminal logs on, the MOD will be displayed.

2. Edit the fields as necessary.
3. Save the changes to the virtual terminal options.

### Setting virtual terminal TSS options

This section describes the steps for setting the virtual terminal Translate Sub-System (TSS) options for a specific IMS.

1. From the Edit IMSID Options panel, type 4 in the selection field and press **Enter**. The IMSID Options – VT TSS Options panel is displayed.

   The following fields are available on this panel:

   - **IMSID**
     - The IMSID of the options module that you selected.
     - This is not an editable field.
   - **TSS table data set name**
     - The name of the TSS library.
     - The TSS library holds the tables that are used by the Translate Subsystem. You can allocate the TSS data set using the Library Format option, the JCL in DLPSAMP member DLP#TSSA, or ISPF utilities. For more information about formatting TSS libraries, see the *DELTA PLUS User Guide*.
     - If you use ISPF for the allocation, the data set should be physical sequential with a RECFM of FS and an LRECL and BLKSIZE of 4096. The space used depends on the amount of data to be contained in the TSS data set; an initial allocation of 1 cylinder is the recommended minimum. If you omit this parameter and any of the virtual terminal exits require TSS, user abend 4060 subcode 010 occurs.
   - **Number of cache buffers**
     - Look-aside buffers are a cache in the extended private area. Translate Subsystem Services store the most recently referenced blocks from the TSS library in the look-aside buffers to speed up TSS response. Valid values are any number from 5 to 1024. For best performance, specify one (for the control record) plus the total number of index and table blocks for all tables (shown on the Table Select panel). To ensure that the most recent data is accessed, all tables must be refreshed. For more information about refreshing TSS libraries, see the *DELTA PLUS User Guide*.

   **Note**

   If you specify a value of 0, the buffers will be eliminated and I/O to the data set will be required each time that table data is needed.
Virtual printers
The name of the TSS table that is used to define the valid virtual printer LTERM names.

Virtual printer timer override
The name of the TSS table that is used to derive Timer facility override values.
Virtual printers that use models defined to IMS with OPTIONS=DISCON are automatically logged off whenever the queue count is zero. The OPTIONS=DISCON parameter takes precedence over the No Automatic Timeout option available through the Virtual Printer Timer Override table.

Unsolicited output
The name of the TSS table that contains the LTERM names that are to be created when a message is sent to an unknown destination.

Warning
This table is the final search to determine whether a destination is valid. Liberal use of wild cards (*) may allow creation of LTERMs that you do not wish to have created.

Virtual remote LTERMs
The name of the TSS table used for the output.
The table must consist of 8-byte argument and function fields. The argument field contains the virtual remote LTERM name and the function field contains the MSNAME of the link to the destination IMS system.

Unsolicited output TRANSACT
The name of the TSS table used to define the valid dynamic transaction names.
The table must consist of 8-byte argument and function fields. The argument field contains a dynamic transaction name and the function field contains the name of an IMSGEN-defined or DELTA List transaction to be used as a model to build the dynamic transaction.

Require ALLROWS keyword on /DIS TSSTABLE command
A / indicates that users must enter the ALLROWS keyword on the /DIS TSSTABLE command to display all entries in the table.
Requiring the ALLROWS keyword on this command prevents inadvertent display of an entire table.

2. Edit the fields as necessary.
3. Save the changes to the TSS options.

Setting virtual terminal logon options
Steps for setting options that are related to the method for obtaining a logon model node name for a specific IMS.
1. From the Edit IMSID Options panel, type 5 in the selection field and press Enter.

The IMSID Options – VT Logon Options panel is displayed.
The following fields are available on this panel:

**IMSID**

The IMSID of the options module that you selected.

This is not an editable field.

**Method**

The method that DELTA PLUS VIRTUAL TERMINAL uses to create node names from logon models.

---

**Note**

Model node names should never exist in the VTAM network. The model names that are specified in the IMSID options for terminals must not be inadvertently or specifically changed by executing a DELTA List. The mask name that is used for adding terminals must not resolve to a terminal that is used as a model.

---

1. **Defaults**
   - **SLU2 logon model node name**
     The name of a terminal that is present in the IMS Stage-1 system definition which DELTA PLUS VIRTUAL TERMINAL can use as a model control block for SLUTYPE2 devices.
     NONE indicates that there are no SLUTYPE2 devices in your network that will be used as virtual terminals.
   - **3270 logon model node name**
     The name of a terminal that is present in the IMS Stage-1 system definition which DELTA PLUS VIRTUAL TERMINAL can use as a model control block for VTAM 3270 devices.
     NONE indicates that there are no VTAM 3270 devices in your network that will be used as virtual terminals.
   - **SLU1 logon model node name**
     The name of a terminal that is present in the IMS Stage-1 system definition which DELTA PLUS VIRTUAL TERMINAL can use as a model control block for SLUTYPE1 devices. A blank value indicates that there are no SLUTYPE1 devices in your network that will be used as virtual terminals.
   - **SLUP logon model node name**
     The name of a terminal that is present in the IMS Stage-1 system definition which DELTA PLUS VIRTUAL TERMINAL can use as a model control block for SLUTYPEP devices. A blank value indicates that there are no SLUTYPEP devices in your network that will be used as virtual terminals.

2. **TSS**
   Indicates that the TSS table that is specified in the TSS table name field will be used to translate the VTAM terminal type and screen size into a logon model node name.

3. **User exit**
   Indicates that a Logon Exit routine in module VTFEXIT n is to be called. This routine provides the name of the logon model.
Unless the table name is hard-coded, the sample exit will use the TSS table name that is specified for Method option 2

2. Edit the fields as necessary and save the changes to the virtual terminal logon options.

Setting virtual terminal signon bypass options

This section describes the steps for setting options that are related to the method for obtaining an LTERM when signon is not required for a specific IMS.

From the Edit IMSID Options panel, type 6 in the selection field and press Enter.

The IMSID Options – VT Signon Bypass Options panel is displayed.

The following fields are available on this panel:

**IMSID**

The IMSID of the options module that you selected.

This is not an editable field.

**Method**

The LTERM name selection method for virtual terminals that are not required to perform an IMS signon.

**Note**

If some users are required to sign on and others are not, enter the following information in the signon bypass TSS table for each user who is not required to sign on:

- The node name
- The associated LTERM

The remainder of the nodes will fail the table search and will be required to sign on.

**Default**

Indicates that the node name will be used as the LTERM name.

**TSS**

Indicates that Translate Subsystem Services (TSS) will translate the node name to an LTERM name.
You can use TSS to translate the derived LTERM name into a virtual terminal Timer facility override value.

This option uses the same logic as the Signon Bypass Exit sample routine that is distributed in exit VTFEXBXX.

**User exit**

Indicates that a signon-bypass exit routine in module VTFEXITn will be called. This exit routine is responsible for providing an LTERM name, and a virtual terminal Timer facility override value.

For more information about the requirements for this exit, see the *DELTA PLUS User Guide*.

**Note**

The sample exit uses the TSS table names that are specified in the Node to LTERM TSS table name and LTERM timer override TSS table name fields.

**Node to LTERM TSS table name**

The name of the TSS table that is used to derive the LTERM name when using the Signon Bypass Exit routine.

A suggested table name is NLTERM.

**LTERM timer override TSS table name**

The name of the TSS table that is used to derive a virtual terminal Timer facility override value.

A suggested table name is LTERMOR.

1. Edit the fields as necessary.
2. Save the changes to the virtual terminal signon bypass options.

**Setting virtual terminal signon options**

This section describes the steps for setting options that are related to the method for obtaining an LTERM when signon is required for a specific IMS.

From the Edit IMSID Options panel, type 7 in the selection field and press Enter.

The IMSID Options – VT Signon Options panel is displayed.

The following fields are available on this panel:

**IMSID**
The IMSID of the options module that you selected.

This is not an editable field.

**Key**

1 Node name

Indicates that the node name is used in the selection technique for permanent LTERMs.

2 Userid

Indicates that the userid is used instead of the node name in the selection technique for permanent LTERMs.

**Method**

The LTERM name selection method for virtual terminals that are required to perform an IMS signon.

1 **Signon-bypass**

Indicates that the LTERM that was created using the Signon Bypass option (specified on the IMSID Options - VT Signon Bypass Options panel) remains the permanent LTERM name.

This option is for users who want to use the Signon Bypass option to establish the LTERM name, but who also have certain user groups that do sign on.

With this option, the AOI exit sees the response to the signon command. As far as DELTA PLUS VIRTUAL TERMINAL is concerned, this is an NOP of virtual terminal signon processing logic in the sense that no action of any kind is taken. No LTERMs are assigned and no conversations are released.

**Note**

The following options assign a permanent LTERM name based on either the node name or the userid, depending on the selection made in the Key field.

2 **Key**

Indicates that an LTERM equivalent to the node name or userid as specified in the Key field is used. No model override or timer override is supplied.

3 **TSS**

Indicates that TSS tables will translate the node name or userid into an LTERM name. The TSS tables then translate the derived LTERM name into a virtual terminal Timer facility override value.
4 User exit

Indicates that a Signon Exit sample routine in module VTFEXITn will be called. This exit routine is responsible for providing an LTERM name and a virtual terminal Timer facility override value.

For more information about the requirements for this exit, see the DELTA PLUS User Guide.

If you select this option and use the Signon Exit sample routine that is provided with DELTA PLUS VIRTUAL TERMINAL, you must also specify values for the Key to LTERM TSS table name and LTERM timer override TSS table name fields.

If you select this option and have installed any of the Signon Exit sample routines that are provided with DELTA PLUS VIRTUAL TERMINAL, the Signon Exit routines determine the LTERM name based on the userid or node name (depending on the value that you specified in the Key field).

Key to LTERM TSS table name

The name of the TSS table that is used to determine the LTERM name.

If the node name is used, a suggested tablename is NLTERM.

If the userid is used, a suggested table name is ULTERM.

LTERM timer override TSS table name

The name of the TSS table that is used to derive a virtual terminal Timer facility override value.

A suggested table name is LTERMOR.

1. Edit the fields as necessary.
2. Save the changes to the virtual terminal signon options.

Setting extended options

This section describes the steps for setting extended options for a specific IMSID.

DELTA PLUS VIRTUAL TERMINAL was designed to function consistently in every IMS system. Occasionally, a feature is added that does not completely fit into the basic design of the product, but it is deemed worthwhile for customers who may have a specific need for that feature. These types of features are known as extended options.

⚠️ Note

Extended options are not required.

The DELTA PLUS VIRTUAL TERMINAL extended options module is named DLA@iii (where iii is the IMSID).
Warning

Extended options are features that have been added to resolve a specific customer need. You should not use these options unless you fully understand the results.

Call BMC Customer Support if you are unsure whether these options will solve the problem that you are trying to address.

To set extended options

1. From the Edit IMSID Options panel, type 8 in the selection field and press Enter.
   The IMSID Options – Extended Options panel is displayed.
   The following fields are available on this panel:
   
   **IMSID**
   The IMSID of the options module that you selected.
   This is not an editable field.
   
   **Use DFS3649A replacement format on sysgen'ned terminals**
   A / indicates that the DFS3649A replacement option for static nodes will be used in addition to virtual terminals.
   
   **Pass VTAM user data**
   A / indicates that VTAM user data will be passed to the logon exit.
   If the Userid and password supplied in VTAM user data field is also selected, the VTAM user data will follow the userid and password. This data will be available to the first call to the IMS greetings message exit.

   **Note**
   This option is incompatible with the Retry signon bypass when initial signon fails option.

   **Pass VTAM user data from logon to signon**
   A / indicates that the VTAM user data will be passed from the logon exit to the signon exit.

   **Note**
   For this option to work, you must also select the Userid and password supplied in VTAM user data option. This option is incompatible with the Retry signon bypass when initial signon fails option.

   **Preserve response mode across signons**
A / indicates that the terminal 'awaiting response' indication for virtual terminals will be preserved from logon to logon.

**Note**
If this option is not selected, the indication is preserved for sysgened terminals, but not for virtual terminals.

/EXIT conversations
A / indicates that conversations from a previous session will be automatically exited. This option takes effect when IMS creates a dynamic terminal that uses an existing LTERM and USER structure that has an active conversation committed to it.

/DEQ messages
A / indicates that all messages from a previous session are automatically dequeued. This option takes effect when IMS creates a dynamic terminal that uses an existing LTERM and USER structure that has one or more messages queued to it.

Use DFS3650I replacement format on sysgened terminals
A / indicates that the DFS3650I replacement option for static nodes will be used in addition to virtual terminals. Bypass RACF authorization for conversations
A / indicates to bypass RACF authorization for conversations. If you select this option, DELTA PLUS VIRTUAL TERMINAL will specify the node name as the user ID that RACF authorization requires. This option will allow you to use the /EXIT conversations option to exit all conversational transactions, regardless of transaction authorization. This option does not allow unauthorized use of any transaction.

/EXIT non-held conversations after held conversation interval
A / indicates to EXIT non-held conversations after the Held conversation exit interval is exceeded. Reset PRESET mode (IMS 7.1 and earlier)
A / indicates that the preset destination mode will be reset at signoff. Use LTERM edit routine DFSCNTE0
A / indicates that a user-supplied LTERM edit routine will be used. Do not delete USRMs and LTERMs at signoff
A / indicates to bypass deletion of CNTs and users at signoff.

**Note**
This option is not compatible with the Do not delete USERS and LTERMS if stopped option.

Retry signon bypass when initial signon fails
A / indicates to retry signon bypass when an initial signon attempt fails.
Note

This option is not compatible with the Pass VTAM user data and Pass VTAM user data from logon to signon options.

Userid and password supplied in VTAM user data

A / indicates that the userid and password will be included in the VTAM user data that is passed to the logon exit.

Ignore DFS3650I replacement message when running ACF2 or Top Secret

A / indicates that the DFS3650I replacement message in message table module VTFSMSG0 will be ignored when running ACF2 or Top Secret security. Call ETO signoff exit DFSSGF0

A / indicates that the ETO signoff exit DFSSGF0 will be loaded during IMS initialization. Call ETO logon exit DFSLGNX0

A / indicates that the ETO logon exit DFSLGNX0 will be called during logon processing. Call ETO logoff exit DFSLGF0

A / indicates that the ETO logoff exit DFSLGF0 will be called during IMS initialization. Allow more than 8 LTERMs per USER

A / indicates that allow more than 8 LTERMs per USER. FID class for /DISPLAY command

A one-character format identifier (FID) class that will identify /DISPLAY command output that is prepared by DELTA PLUS when presented to an AOI program. The default value is 

#Enable DELTA PLUS VT compatibility with session managers

A / indicates that if you are using a session manager, the real VTAM node name for these terminals will be used instead of the session manager pool node name.

Note

The following prerequisites must be met in order to use this option:

- The session manager product must place the real VTAM node name in the VTAM user data field when a terminal user logs on. Check with your local session manager support group or the session manager vendor to determine whether your product complies.
- The VTAM APPL for this IMS must have PARSESS=YES.

To specify the session manager pool node names to be used in conjunction with this option, use the Prefixes for session manager node names fields. VTAM user data contains trailing blanks

A / indicates that any 'OPNDST NODE nodename USER username' command will create the nodename as the username if your VTAM user data contains trailing blanks immediately following the node name. Prefixes for session manager node names
The user-defined prefix(es) for session manager node names to be used in conjunction with the Enable DELTA PLUS/VT compatibility with session managers option. Specify ALL to process all dynamic nodes.

2. Edit the fields as necessary.
3. Save the changes to the extended options.

### Refreshing TSS tables

This section describes the steps for clearing the TSS cache buffers if you are using cache buffering to access TSS table data.

Clearing the cache buffers causes DELTA PLUS VIRTUAL TERMINAL to load the most current information the next time a table is accessed.

⚠️ **Note**

This process only applies to changing your options while IMS is up. If IMS is not up, the refresh process is not needed since changes will take effect after the next restart.

#### To refresh the TSS tables

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing the products from an ISPF options menu (see page 57) or through the CLIST that you created in Accessing the products from a CLIST (see page 57).
   The Main Menu is displayed.
2. Type 4 in the selection field and press **Enter**.
   The Administration Menu is displayed.
3. Type 5 in the selection field and press **Enter**.
   The Refresh Menu is displayed.
4. Type 2 in the selection field.
5. Perform one of the following actions:
   - To update the TSS tables for a single IMS system, type an IMSID in the **IMSID or Group** field.
   - To update the TSS tables for multiple IMS systems, type a Group name in the **IMSID or Group** field.
   Press **Enter**.
   The Confirm TSS Refresh pop-up window is displayed.
6. Type 1 in the selection field and press **Enter**.
   DELTA PLUS VIRTUAL TERMINAL refreshes the TSS tables and the TSS Refresh Results pop-up window is displayed.
7. Press **F3** to exit the TSS Refresh Results pop-up window.
Starting products

You must start the products after you complete the other configuration tasks that are described in this section.

To start the products

1. Update the IMS control or DBCTL region, if applicable, to include the APF-authorized library in the STEPLIB concatenation. The APF-authorized library must precede the IMS RESLIB in the STEPLIB concatenation.

   **Note**
   
   BMC recommends that you execute the IMS system from a STEPLIB or JOBLIB. If it is unacceptable at your site to execute IMS from a STEPLIB or JOBLIB, you must use ddname BMCRESLB to allocate the IMS RESLIB that is accessed from the LINKLIST to IMS. In addition, the DELTA PLUS APF-authorized library must be in the BMCRESLB concatenation.

2. Start BMCXLINK.
   
   BMCXLINK allows users to communicate with an IMS system. TSO-based users of IMS and the product do not have to run on the same CPU. DLPCNTL member DLP#LINK provides sample JCL for BMCXLINK.

   **Note**
   
   The BMCXLINK task must have WRITE access authority to the Log and History File data sets.

3. Process the CPU ID password (either bypass or permanent) that will allow the product to work.

   For more information, see the installation guide.

4. Cold start IMS.

DELTA PLUS VIRTUAL TERMINAL customization worksheet

Refer to the following worksheet as you work through the customization process for DELTA PLUS VIRTUAL TERMINAL.
<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Update IMS and VTAM.</td>
<td>Updating IMS (see page 54)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating VTAM in DLA and DLP (see page 54)</td>
</tr>
<tr>
<td>2.</td>
<td>Provide access to the ISPF interface through a CLIST or through an ISPF options menu.</td>
<td>• Adding the products to TSO/ISPF (see page 56)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accessing the products from a CLIST (see page 57)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accessing the products from an ISPF options menu (see page 57)</td>
</tr>
<tr>
<td>3.</td>
<td>Limit access to DELTA PLUS VIRTUAL TERMINAL through user access profiles, a SAF interface to RACF, or TopSecret.</td>
<td>• Limiting access to the products (see page 59)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implementing user access profiles and UPF security (see page 60)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implementing a SAF interface to RACF (or equivalent) product (see page 67)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implementing TopSecret (see page 70)</td>
</tr>
<tr>
<td>4.</td>
<td>Set global options.</td>
<td>Setting global options in DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL (see page 71)</td>
</tr>
<tr>
<td>5.</td>
<td>Set IMSID options for each control region that DELTA PLUS VIRTUAL TERMINAL services.</td>
<td>Setting IMSID options when installing DELTA PLUS or DELTA PLUS VIRTUAL TERMINAL (see page 75)</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the functionality of the FDR feature.</td>
<td>Enabling the FDR feature (DELTA PLUS and DELTA PLUS VIRTUAL TERMINAL) (see page 82)</td>
</tr>
<tr>
<td>7.</td>
<td><strong>(optional)</strong> Set Group options.</td>
<td>Setting Group options (see page 83)</td>
</tr>
<tr>
<td>8.</td>
<td>Refresh the CPUID options.</td>
<td>Refreshing CPUID options (see page 87)</td>
</tr>
<tr>
<td>9.</td>
<td>Create and format the Log and History File data sets.</td>
<td>Creating and formatting Log and History File data sets (see page 88)</td>
</tr>
<tr>
<td>10.</td>
<td>If you are installing DELTA PLUS at your site for the first time, create View Profiles.</td>
<td>Creating View Profiles (see page 90)</td>
</tr>
<tr>
<td>11.</td>
<td>Edit the View Profiles.</td>
<td>Editing View Profiles (see page 96)</td>
</tr>
<tr>
<td>12.</td>
<td>Allocate new data sets.</td>
<td>Allocating new data sets (see page 104)</td>
</tr>
<tr>
<td>13.</td>
<td><strong>(optional)</strong> Add IMSIDs to existing Groups' Log data sets.</td>
<td>Adding an IMSID to an existing Group’s Log data sets</td>
</tr>
<tr>
<td>14.</td>
<td>Complete DELTA PLUS VIRTUAL TERMINAL customization.</td>
<td>• Enabling DELTA PLUS VIRTUAL TERMINAL (see page 109)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Setting virtual terminal IMSID options (see page 109)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Refreshing TSS tables (see page 126)</td>
</tr>
<tr>
<td></td>
<td>Start DELTA PLUS.</td>
<td>Starting products (see page 127)</td>
</tr>
</tbody>
</table>
Customizing Energizer for IMS Connect

This section describes customization tasks that are unique to Energizer for IMS Connect. Customizing refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered in this section:

- Overview of customizing Energizer for IMS Connect (see page 129)
- Energizer for IMS Connect customization worksheet (see page 129)
- Adding Energizer to TSO/ISPF (see page 130)
- Completing Energizer implementation (see page 134)
- Adding BMC security (see page 136)
- Archiving journal data sets automatically (see page 137)

Overview of customizing Energizer for IMS Connect

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and customizing the product libraries, see the Installation System documentation.

The customization tasks in this section are unique to Energizer.

Energizer for IMS Connect customization worksheet

Refer to the following worksheet as you work through the customization process.

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Provide access to</td>
<td>1. Provide access to the ISPF interface through a CLIST or through</td>
<td>• Adding Energizer to TSO/ISPF (see page 130)</td>
</tr>
<tr>
<td>the ISPF interface</td>
<td>an ISPF options menu.</td>
<td>• Accessing Energizer from a CLIST (see page 130)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accessing Energizer from an ISPF options menu (see page 130)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Using the Energizer ISPF interface (see page 132)</td>
</tr>
</tbody>
</table>
Adding Energizer to TSO/ISPF

This section describes the procedures for adding Energizer to TSO/ISPF.

You can customize the online interface so that you can invoke it from a CLIST or from an ISPF options menu. For more information, see Accessing Energizer from a CLIST (see page 130) and Accessing Energizer from an ISPF options menu (see page 130).

Accessing Energizer from a CLIST

A sample CLIST that provides access to the online interface using LIBDEF is available in the SAMP library. You can copy member IPRCI@00 of the SAMP library into your CLIST library and update the following data set names to reference your data sets:

- &IPRLIB
- &IPRMLIB
- &IPRPLIB
- &IPRTLIB
- &IPRREXX

Accessing Energizer from an ISPF options menu

Accessing Energizer from an ISPF options menu requires that you pre-allocate the necessary ISPF data sets to the user.

You must add the following libraries to the TSO logon procedure for each user who requires access to Energizer:

- Load library (ISPLLIB)
- Panel library (ISPLLIB)
- Message library (ISPMLIB)
- Table library (ISPTLIB)
Energizer contains a hidden panel that allows you to specify many ISPF default product values. The panel is located in member IPRPUSER of the IPRPLIB library. Review the member to customize the ISPF interface default values for the product. Comments are included in the member to assist you.

The following figure shows a sample ISPF/PDF Primary Option Menu that has been modified to access Energizer.

**Sample modifications to ISPF/PDF Primary Option Menu**

```plaintext
%-----------------------  ISPF/PDF PRIMARY OPTION MENU  -----------------
%OPTION  ===>                                                           +
%  0  +ISPF PARMS  - Specify terminal and user parameters
%  1  +BROWSE     - Display source data or output listings
%  2  +EDIT       - Create or change source data
%  3  +UTILITIES  - Perform utility functions
%  4  +FOREGROUND - Invoke language processors in foreground
%  5  +BATCH      - Submit job for language processing
%  6  +COMMAND    - Enter TSO command or CLIST
%  7  +DIALOG TEST - Perform dialog testing
%  C  +CHANGES    - Display summary of changes for this release
%  E  +Energizer  - Energizer for IMS Connect
%  Q  +SDSF       - Spool Display and Search Facility
%  S  +SMP/E      - New Version of SMP
%  T  +TUTORIAL   - Display information about ISPF/PDF
%  X  +EXIT       - Terminate ISPF using log and list defaults
%+Enter%END+command to terminate ISPF.
%
}INIT
.
HELP = ISR00003
&ZPRIM = YES /* ALWAYS A PRIMARY OPTION MENU */
&ZHTOP = ISR00003 /* TUTORIAL TABLE OF CONTENTS */
&ZHINDEX = ISR91000 /* TUTORIAL INDEX - 1ST PAGE */
}PROC
&ZSEL = TRANS( TRUNC (&ZCMD, ',')
  0,'PANEL(ISPOPTA)'
  1,'PGM(ISRBRO)'
  2,'PGM(ISREDIT)'
  3,'PANEL(ISRUTIL)'
  4,'PANEL(ISRFP)'
  5,'PGM(ISRJB1) PARM(ISJRPA) NOCHECK'
  6,'PANEL(ISRTSOT)'
  7,'PGM(ISRYXDR) NOCHECK'
 C,'PGM(ISPTUTOR) PARM(ISR00005)'
 E,'CMD(IPRCI@000) NEWAPPL(IPR1)'
 Q,'PANEL(ZSDSFOPT) NEWAPPL(ISF)'
 S,'PGM(GIMISCV) PARM(&ZCMD) NEWAPPL(SMP2)'
 T,'PGM(ISPTUTOR) PARM(ISR00000)'
 ,',',
```

BMC Software Confidential
Using the Energizer ISPF interface

The console and UIM server are not required to run the ISPF version of Energizer; however, any changes that you make to the options library or its members will affect users who run Energizer with the console interface within the same sysplex.

Note

The UIM server resides on the mainframe and handles communication between the console and BMC console-enabled mainframe products and features.

The console is the graphical user interface (GUI). The console runs on a client workstation under the Microsoft Windows operating system and communicates with the UIM server through TCP/IP technology.

For more information about the UIM server and the console, see Customizing the console (see page 227)

For information about the Energizer ISPF interface functions and how they work, see the Energizer for IMS Connect User Guide. For information about an ISPF panel, see the online Help.

Creating eLinks

An eLink is the Energizer address space that provides the communications between the UIM server, the operator console, and the IMS Connects.

You do not need an eLink or an eLink started task to use the ISPF or console interfaces. You only need an eLink to be able to enter Energizer commands from an z/OS operator console.

If you intend to run Energizer without running an eLink address space, you must specify the host name and port number to the options for each IMS Connect that is defined to Energizer. Without the host name and port number, the Database Console cannot communicate with the IMS
Connect. You can add the host name and port number by using the IMS Connect Options panel in the Energizer ISPF interface. You can activate the changes by reloading the IMS Connect options from the ISPF interface, or by clicking **Save and Reload** in the Edit Configuration - General Tab of the Database Console.

For more information, see the *Energizer for IMS Connect User Guide*.

**Securing access to the Energizer ISPF interface**

The IPRCMDS0 exit is required to process Energizer commands when you use the Energizer ISPF interface.

1. On the IPRCMDS0 Virtual Exit panel, change the IPRCMDS0 virtual exit as follows:
   - Make **Password** a required field
   - Select **Enable userid authentication**
   - Select **Enable IMS Connect authentication**
   - Select **Enable transaction authentication**
   - Specify an **IMS Connect resource**

**Excerpt from IPRCMDS0 Virtual Exit panel**

```
<table>
<thead>
<tr>
<th>IRM security fields</th>
<th>Offset Status (offset=0 for default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Userid . . . . . . .</td>
<td>0____ REQUIRED (Always required)</td>
</tr>
<tr>
<td>Group . . . . . . .</td>
<td>0____ OPTIONAL (REQUIRED or OPTIONAL or NONE)</td>
</tr>
<tr>
<td>Password . . . . . .</td>
<td>0____ REQUIRED (REQUIRED or OPTIONAL or NONE)</td>
</tr>
<tr>
<td>New password . . .</td>
<td>0____ OPTIONAL (OPTIONAL or NONE)</td>
</tr>
</tbody>
</table>
```

Select (type a '/') any of the following.

/ Enable userid authentication
/ Enable IMS Connect authentication
/ Enable transaction authentication

**IMS Connect resource . NAME____ (used for IMS Connect authentication)**

2. Ensure that the options for any IMS Connects that need to be secured have a security class name and, optionally, a resource prefix.

3. Create resource rules in the appropriate security class for the following resources (where **rprefix** is the prefix from the IMS Connect options and **connres** is the IMS Connect resource from the IPRCMDS0 exit):

<table>
<thead>
<tr>
<th>Resource</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>rprefix.connres</td>
<td>Overall access to the IMS Connect</td>
</tr>
<tr>
<td>rprefix.-DIS</td>
<td>Access to display commands (ISPF options 2 and 3)</td>
</tr>
<tr>
<td>rprefix.-SET</td>
<td>Access to set commands (ISPF option 3)</td>
</tr>
<tr>
<td>rprefix.-REL</td>
<td>Access to reload commands (ISPF options 1 and 3)</td>
</tr>
<tr>
<td>rprefix.-RES</td>
<td>Access to reset commands (ISPF option 3)</td>
</tr>
</tbody>
</table>
### Completing Energizer implementation

To complete implementation of Energizer, perform the following steps:

1. Edit member IPR#OPTS of the IPRCNTL library and allocate the IPROPTS data set.
2. Determine whether to use Dynamic Journaling or static journal data sets.
   - With Dynamic Journaling, Energizer allocates new journal data sets as needed, instead of reusing (writing over the data in) a set of existing journal data sets. If you choose to use Dynamic Journaling, you will specify the appropriate Dynamic Journaling options when you define each IMS Connect to Energizer. For more information, see the *Energizer for IMS Connect User Guide*.
   - With static journal data sets, Energizer reuses (writes over the data in) a set of previously allocated journal data sets. If you choose to use static journal data sets, edit member IPR#JRNA of the IPRCNTL library:
     - Allocate the required journal data sets for the eLink started task.
     - Allocate the required journal data sets for the IMS Connect started task.
3. If you are using static journal data sets, using the eLink started task that was created when you specified Energizer options, update the eLink Journal 1-8 DD statements to reflect the journal data sets that were allocated with the IPR#JRNA JCL. The data set that you specified in the *UIM Customized Parm library* field on the UIM server Middleware Options panel contains the eLink member that was created during installation. For more information about specifying the Energizer options, see the installation guide.
4. If you are using static journal data sets, update the IMS Connect started task with the journal data sets that were allocated with member IPR#JRNA.
5. Update VTAM.
   - The following figure shows sample VTAM statements. Sample statements are also available in member IPR$APPL of the IPRSAMP library.
     - a. Create an APPL statement for the following started tasks:
        - Each Energizer started task that is defined

---

<table>
<thead>
<tr>
<th>Resource</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>rprefix.-EXEC</td>
<td>Access to IMS Connect commands (ISPF option 3)</td>
</tr>
</tbody>
</table>

When you have completed steps Step 1 (see page 133) through Step 3 (see page 133), ISPF users are prompted for a password which is authenticated within IMS Connect.

⚠️ **Note**

If **Password** is an optional field, it still validates against the user ID.

You can abbreviate Energizer and IMS commands to three characters. To protect all forms of the command, write rules such as `rprefix.-EXE*`. 
5. Each UIM server started task that is defined

Note

VTAM LU names must be unique throughout your VTAM network.

Sample Energizer and UIM server APPL statements

<table>
<thead>
<tr>
<th>IPRELINK APPL AUTH=(ACQ, PASS), MODETAB=IPRMODE, DLOGMOD=IPRMOD1, EAS=5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPRICONS APPL AUTH=(ACQ, PASS), MODETAB=IPRMODE, DLOGMOD=IPRMOD1, EAS=5</td>
</tr>
</tbody>
</table>

b. Verify that the SYS1.VTAMLST (or equivalent) member names, LU names, and ACBNAMEs that you created conform to your site’s standards and specify the Energizer product requirements.

c. If you have the required authority, activate the VTAM definition statements; otherwise, verify that the definitions have been activated before proceeding.

6. Copy the UIM server started task into your SYSx.PROCLIB data set.

Note

You must complete this step before you can start the UIM server.

The UIM server started task is located in the data set that you specified in the UIM Customized Parm library field on the UIM server Middleware Options panel. The started task name is the name that you specified during installation.

7. If required to run eLink, copy the eLink started task name into your SYSx.PROCLIB data set.

Note

You must complete this step before you can start eLink.

The eLink started task is located in the data set that you specified in the UIM Customized Parm library field on the UIM server Middleware Options panel. The started task name is the name that you specified during installation. For information about specifying the started task name, see the installation guide.

8. Perform the following tasks for each IMS Connect that Energizer uses:
a. Add the Energizer load library (IPRLIB) to the IMS Connect STEPLIB concatenation. Ensure that the Energizer library is the first library in the concatenation, and ensure that the library is APF-authorized.

b. Add the IPROPTS DD statement to your IMS Connect started task JCL. IPROPTS is the options data set that you specified during installation. For more information, see the installation guide.

c. If you are using static journal data sets, add the journal DD statements to your IMS Connect started task JCL.

---

**Note**

This step is required if you intend to enable the journal function within IMS Connect and you are using static journal data sets. It does not apply if you are using Dynamic Journaling.

---

9. *(optional, unless routing)* Add the Energizer load library to each IMS control region STEPLIB concatenation that uses Energizer. Ensure that the Energizer library is the first library in the concatenation, and ensure that the library is APF-authorized.

10. *(optional, unless routing)* Add the IPROPTS DD statement to your IMS control region started task JCL. IPROPTS is the options data set that you specified during installation. For more information, see the installation guide.

11. Start the UIM server started task. For more information, see Operating the UIM server (see page 234)

12. Start the console. For more information, see Customizing the console (see page 227)

---

**Warning**

Do not start eLink or IMS Connect address spaces now. The Energizer options must be defined and saved to the options library. All Energizer configuration must be performed within the console or the ISPF interface.

---

**Adding BMC security**

Before starting IMS Connect, Energizer must be authorized within the IMS Connect address space.

If Energizer is not authorized, IMS Connect abends at initialization.

1. Apply the product password to generate a valid password module. For information about the password security feature, see the installation guide
2. Apply the password that was supplied by your BMC sales representative. Use the sample JCL in member IPR#CPUM of the IPRCNTL library.

The STEPLIB and SYSLIB DD statements are as follows:

```plaintext
//STEPLIB DD DISP=SHR,DSN=BMC.PRODUCT.LOAD <== Ensure IPRSEC3B is in this library
//SYSLIB DD DSN=BMC.PRODUCT.LOAD,DISP=SHR <== PRODUCT LOAD LIBRARY
```

The product load library (IPRLIB) is the library that you created and are using as the STEPLIB data set within your IMS Connect started task.

### Archiving journal data sets automatically

You can set up a batch archive utility to use with Energizer Dynamic Journaling.

To use the Archive utility, you create skeleton JCL that archives a journal. Energizer automatically submits this archive job when Energizer closes and switches a journal.

The following types of journals are not eligible for processing with the Archive utility:

- Static journal data sets
  These data sets are also known as round-robin data sets. They are defined by using the JOURNAL DD statement.
- Dynamic Journaling data sets that do not have the suffix defined by Energizer

These data sets are journals that Energizer has created when the **Append the default suffix (.D yyyydd.mmssst.nn)** option is not selected.

For more information about the Archive utility, see the *Energizer for IMS Connect User Guide*.

### To archive journal data sets automatically

1. For each IMS Connect, specify the options that enable Dynamic Journaling.
   Ensure that the **Append the default suffix (.D yyyydd.mmssst.nn)** option is selected.
2. In a data set that is included in the IMS Connect PROCLIB concatenation, create a skeleton member named ARCHJCL.
   If the ARCHJCL member is not included in the IMS Connect PROCLIB, the Archive utility is disabled.
3. In the ARCHJCL member, specify the appropriate statements to use the Archive utility in your environment.
   For an example, see member IPR#ARCH in the IMCNTL or IPRCNTL data set. The archive job can have multiple steps or it can have a single archive step.
Customizing EXTENDED TERMINAL ASSIST PLUS

This section describes configuration tasks that are unique to the EXTENDED TERMINAL ASSIST PLUS product. *Customizing* refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered in this section:

- Overview of customizing Extended Terminal Assist Plus (see page 138)
- EXTENDED TERMINAL ASSIST PLUS customization worksheet (see page 139)
- Running ETA without ETO (see page 139)
- Updating VTAM (ETA) (see page 141)
- Adding ETA to TSO/ISPF (see page 143)
- Limiting access to ETA (see page 145)
- Setting global options in ETA (see page 153)
- Setting IMSID options for ETA (see page 156)
- Setting TSS IMSID options (see page 160)
- Setting Group options for ETA (see page 162)
- Starting ETA (see page 164)

Overview of customizing Extended Terminal Assist Plus

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and configuring the product libraries, see the Installation System documentation.

⚠️ **Note**

No configuration tasks were performed for ETA.

The customization tasks that are presented in this section are unique to ETA.
EXTENDED TERMINAL ASSIST PLUS customization worksheet

Refer to the following worksheet as you work through the customization process for ETA.

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. <em>(optional)</em> Set up ETA to run without ETO.</td>
<td>Running ETA without ETO (see page 139)</td>
</tr>
<tr>
<td></td>
<td>Update VTAM.</td>
<td>Updating VTAM (ETA) (see page 141)</td>
</tr>
</tbody>
</table>
|      | 2. Provide access to the ISPF interface through a CLIST or through an ISPF options menu. | • Adding ETA to TSO/ISPF (see page 143)  
• Accessing ETA from a CLIST (see page 143)  
• Accessing ETA from an ISPF options menu (see page 144) |
|      | 3. Limit access to ETA through user access profiles or a SAF interface to RACF. | • Limiting access to ETA (see page 145)  
• Implementing user access profiles and UPF security1 (see page 147)  
• Implementing a SAF interface to RACF (or equivalent) product1 (see page 150) |
|      | 4. Set global options.                                               | Setting global options in ETA (see page 153)              |
|      | 5. Set IMSID options for each control region that ETA services.      | Setting IMSID options for ETA (see page 156)              |
|      | 6. If you plan to use the ETA TSS feature, set TSS IMSID options.    | Setting TSS IMSID options (see page 160)                  |
|      | 7. *(optional)* Set Group options.                                   | Setting Group options for ETA (see page 162)              |
|      | 8. Start ETA.                                                        | Starting ETA (see page 164)                               |

Running ETA without ETO

ETA no longer requires use of the IMS Extended Terminal Option (ETO) feature.

If you choose to run ETA without ETO, choose the appropriate procedure for your situation:

- If you are running ETA with ETO and want to discontinue use of ETO, use the To discontinue using ETO with ETA (see page 140) procedure.
By completing this procedure, you no longer need to install the ETO FMID that IBM packages with IMS. You can also discontinue your license for ETO.

- If you have never used ETA with ETO and you do not want to use ETO, use the To configure ETA to run without ETO (see page 140) procedure.

By completing this procedure, you do not need a license for ETO. You do not need to install the ETO FMID that IBM packages with IMS.

To discontinue using ETO with ETA

1. In your IMS procedure library (IMS.PROCLIB), create an ETANDSCx member by copying your existing DFSDSCMx member.
   In these member names, x is the nucleus suffix.
2. In the DFSPBxxx member, disable ETO by changing ETO=Y to ETO=N.
3. Restart IMS.
   You can use any type of restart. ETO is inactive when the restart completes.
4. Verify that ETA started successfully without ETO by checking ETA messages in the IMS control region:
   - The following messages are examples that indicate successful ETA startup:

```
BMCETA258620E NO ERRORS encountered in IMS PROCLIB member ETANDSCx
BMCETA005358I Extended Terminal Assist Plus RESTART complete
```

   - The following messages are examples that indicate configuration issues:

```
BMCETA258620E ERRORS encountered in IMS PROCLIB member ETANDSCx
BMCETA258659E Invalid Descriptor Type x; ignored
```

**Note**

If you encounter a problem, check for errors in the ETANDSCx member, try to correct them, and restart IMS.

If you cannot solve the problem, contact BMC Customer Support. You can reactivate ETO by changing ETO=N to ETO=Y in the DFSPBxxx member and restarting IMS.

5. Verify that ETA functions normally without ETO.
6. *(optional)* Remove the ETO FMID from your SMPE environment.
   As an alternative to this step, you can simply choose not to order the ETO feature with your next IMS upgrade.
To configure ETA to run without ETO

1. In your IMS procedure library (IMS.PROCLIB), create an ETANDSC\textsubscript{x} member by copying your existing DFSDSCM \textsubscript{x} member.
   In these member names, \textsubscript{x} is the nucleus suffix.
2. In the DFSPB\textsubscript{xxx} member, ensure that \textbf{ETO=N} is specified.
3. Start IMS.
   You can use any type of restart.
4. Verify that ETA started successfully by checking ETA messages in the IMS control region:
   - The following messages are examples that indicate successful ETA startup:
     
     ```
     BMCETA258620E NO ERRORS encountered in IMS PROCLIB member ETANDSC\textsubscript{x}
     BMCETA005358I Extended Terminal Assist Plus RESTART complete
     ```
   - The following messages are examples that indicate configuration issues:
     
     ```
     BMCETA258620E ERRORS encountered in IMS PROCLIB member ETANDSC\textsubscript{x}
     BMCETA258659E Invalid Descriptor Type \textsubscript{x}; ignored
     ```
5. Verify that ETA functions normally.

Updating VTAM (ETA)

This section describes the steps you must complete to update VTAM.

⚠️ Note

If you want to base your VTAM definition statements on BMC-provided sample statements, use the sample statements from member ETA$APPL of the ETASAMP library.

1. Assemble and link-edit the VTAM mode table.
   The VTAM mode table is supplied in member ETA#MODE of the ETACNTL library. You must assemble and link-edit the mode table into SYS1.VTAMLIB or its equivalent.
2. Create TSO/ISPF APPL definition statements in SYS1.VTAMLST for each TSO system that will run the product online interface.
   Use the following guidelines when you create TSO/ISPF APPL definition statements:
   - TSO LU names must be unique throughout your VTAM network.
   - TSO ACBNAMEs must be unique only within a given MVS system.
2. **TSO ACBNAMEs** must use the format `prefnnnn` (where `pref` is a four-character prefix used for all BMCXLINK ACBNAMEs and `nnnn` is a number in a sequence that starts with 0001).

   - BMC recommends that the TSO session identifier that begins each TSO/ISPF APPL definition statement match the corresponding TSO ACBNAME; however, a match is *not required.*

   The following figure shows sample statements. Sample VTAM statements are also available in member ETA$APPL of the ETASAMP library.

   **Sample TSO/ISPF APPL statements**

   ```
   ETAU0001  APPL  AUTH=(ACQ,PASS),MODETAB=ETAMODE, X
               DLOGMOD=ETAMOD1,EAS=1,       X
               ACBNAME=ETAU0001
   ETAU0002  APPL  AUTH=(ACQ,PASS),MODETAB=ETAMODE, X
               DLOGMOD=ETAMOD1,EAS=1,       X
               ACBNAME=ETAU0002
   ETAU0003  APPL  AUTH=(ACQ,PASS),MODETAB=ETAMODE, X
               DLOGMOD=ETAMOD1,EAS=1,       X
               ACBNAME=ETAU0003
   ETAU0004  APPL  AUTH=(ACQ,PASS),MODETAB=ETAMODE, X
               DLOGMOD=ETAMOD1,EAS=1,       X
               ACBNAME=ETAU0004
   ETAU0005  APPL  AUTH=(ACQ,PASS),MODETAB=ETAMODE, X
               DLOGMOD=ETAMOD1,EAS=1,       X
               ACBNAME=ETAU0005
   ```

   Create one BMCXLINK APPL statement for each BMCXLINK started task that you will use. **BMCXLINK LU NAMES** must be unique throughout your VTAM network. Sample TSO/ISPF APPL statements (see page 142) shows a sample statement.

   **Sample BMCXLINK APPL statement for ETA**

   ```
   BMCALINK APPL AUTH=(ACQ,PASS),EAS=10
   ```

   **Note**

   One BMCXLINK can be used to service all IMS systems in the entire XCF complex. The only restriction is that if you are using Groups, a single BMCXLINK must be used for all requests against a Group.

3. **Create CDRSC statements if necessary.**

<table>
<thead>
<tr>
<th>If the online interface and BMCXLINK</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run on the same MVS system</td>
<td>Go to Step 4 (see page 143).</td>
</tr>
<tr>
<td>Do not run on the same MVS system in some or all cases</td>
<td></td>
</tr>
</tbody>
</table>
Follow these guidelines when creating CDRSC statements:

- Each CDRSC LU name must match the LU name of the BMCXLINK APPL statement that defines the BMCXLINK task for the IMS system.
- The CDRM= parameter must identify the minor node where the BMCXLINK task and IMS system will run.

The following figure shows sample statements.

**Sample CDRSC definition for MVST system**

<table>
<thead>
<tr>
<th>VBUILD TYPE=CDRSC</th>
<th>ETAL0001 CDRSC CDRM=cdrmid</th>
</tr>
</thead>
<tbody>
<tr>
<td>VBUILD TYPE=CDRSC</td>
<td>ETAL0002 CDRSC CDRM=cdrmid</td>
</tr>
</tbody>
</table>

4. Verify that the SYS1.VTAMLST member names, LU names, and ACBNAMEs that you created conform to your site’s standards and the requirements that are specified in this task.

5. If you want to use the ETA session manager true nodename support feature, verify that the PARSESS=YES parameter is used in the APPL statement for each IMSID on which you want to use the feature.

6. If you have the required authority, activate the VTAM definition statements. Otherwise, verify that the definitions have been activated before proceeding with the configuration process.

---

**Adding ETA to TSO/ISPF**

This section describes the procedures for adding ETA to TSO/ISPF.

You can install the online interface so that you can invoke it from a CLIST or from an ISPF options menu. For more information, see Accessing ETA from a CLIST (see page 143) and Accessing ETA from an ISPF options menu (see page 144).

**Accessing ETA from a CLIST**

A sample CLIST that provides access to the online interface using LIBDEF is available in the SAMP library.

You can copy member ETACI@00 of the SAMP library into your CLIST library and update the following data set names to reference your data sets:

- &ETALLIB
- &ETAMLIB
- &ETAPLIB
Accessing ETA from an ISPF options menu

Accessing ETA from an ISPF options menu requires that you pre-allocate the necessary ISPF data sets to the user.

You must add the following libraries to the TSO logon procedure for each user who requires access to ETA:

- Load library (ISPLLIB)
- ISPF panel library (ISPPLIB)
- ISPF message library (ISPMLIB)
- ISPF table library (ISPTLIB)

ETA contains a hidden panel that allows you to specify many ISPF default product values. The hidden panel is located in member ETAZUSER of the ETAPLIB library. Review the member to customize the ISPF interface default values for ETA. Comments are included in the member to assist you.

The following figure shows a sample ISPF/PDF Primary Option Menu that has been modified to access ETA.

Sample modifications to ISPF/PDF Primary Option Menu

| %----------------------- | ISPF/PDF PRIMARY OPTION MENU | ---| --- |
| %OPTION | ISPF/PDF PRIMARY OPTION MENU | 0 | 0 |
| % | ISPF/PDF PRIMARY OPTION MENU | 1 | 1 |
| % | ISPF/PDF PRIMARY OPTION MENU | 2 | 2 |
| % | ISPF/PDF PRIMARY OPTION MENU | 3 | 3 |
| % | ISPF/PDF PRIMARY OPTION MENU | 4 | 4 |
| % | ISPF/PDF PRIMARY OPTION MENU | 5 | 5 |
| % | ISPF/PDF PRIMARY OPTION MENU | 6 | 6 |
| % | ISPF/PDF PRIMARY OPTION MENU | 7 | 7 |
| % | ISPF/PDF PRIMARY OPTION MENU | C | C |
| % | ISPF/PDF PRIMARY OPTION MENU | E | E |
| % | ISPF/PDF PRIMARY OPTION MENU | Q | Q |

- Specify terminal and user parameters
- Display source data or output listings
- Create or change source data
- Perform utility functions
- Invoke language processors in foreground
- Submit job for language processing
- Enter TSO command or CLIST
- Perform dialog testing
- Display summary of changes for this release
- EXTENDED TERMINAL ASSIST PLUS
- Spool Display and Search Facility
Limiting access to ETA

This section describes the procedures for limiting access to ETA.

By default, access to many ETA functions is unlimited. To restrict product usage, you must take steps to protect the functions that you want to restrict.

Under most circumstances, you do not have to set security when initially installing ETA. Therefore, you may want to defer setting security until you have reviewed the various security methods.

ETA allows you to secure product features through either of the following methods:

- User access profiles
If you decide to secure product features through user access profiles, you must first establish administrator authority to create and change user access profiles. After you establish administrator authority for appropriate users, you can use UPF security to create and maintain user access profiles. For more information about establishing administrator authority and using UPF, see Implementing user access profiles and UPF security1 (see page 147).

- A System Authorization Facility (SAF) interface to RACF or an equivalent product
  For more information about securing product features through a SAF interface, see Implementing a SAF interface to RACF (or equivalent) product1 (see page 150).

**Note**

If you are going to restrict access to product functions via the SAF security interface, you must define the ACTIVATE resource before SAF will activate. The ACTIVATE resource provides a method to quickly activate and deactivate the interface. Users must have READ access to the ACTIVATE resource to access the product main menu. You should not define the ACTIVATE resource until you define all other resources.

**Warning**

If your site is running ACF2 Version 1.6.0 or later and you elect not to install the SAF security interface, you must add the following SAFDEF entry to your ACF2 parameters:

```plaintext
FUNCTION(4) FUNCRSN(0) ID(product) MODE(IGNORE)
RACROUTE(REQUEST=AUTH CLASS=prd#) RETCODE(4)
```

Failure to add this SAFDEF entry may cause you to receive the following error message when attempting to perform any product function:

```
BMCprdnnnnnn NOT AUTHORIZED TO USE product
```

Adding this SAFDEF entry will ensure that your existing internal product security will be used. If you decide to use the SAF security interface at a later time, you must delete this SAFDEF entry from your ACF2 parameters.

Unless you use one of these methods to control use of product features, access to ETA and use of its features is effectively unlimited. The approaches to internal security are mutually exclusive.
Implementing user access profiles and UPF security

By default, user access profiles determine which product features a user is authorized to use on a specific IMS system.

The UPF data set is used to maintain user access profiles. A user access profile is the user ID’s authorization for an IMSID. All product functions that reference an IMS control region require specification of the control region’s IMSID. Before a user may designate an IMSID, a user access profile must exist for the user ID and IMSID combination.

Administrator authority is required to create and maintain user access profiles. Unless you establish administrator authority for appropriate users, access to product features is effectively unlimited: all users are authorized to create user access profiles, so all users can authorize themselves to use all product features. BMC recommends that you establish administrator authority for appropriate personnel and restrict the use of product features, as appropriate, by creating user access profiles.

You can establish administrator authority for users with either of the following methods:

- **User ID list**
  You can create a list of user IDs that have administrator authority for creating and modifying user access profiles. Member ETMXUID0 of the ETASAMP library contains a sample user ID list that you can modify for your facility.

  The following guidelines apply to creating the user ID list:
  - The user ID list allows generic parameters. That is, only the specified characters in the user ID are matched. The SAMP library member provides information about using generic parameters.
  - Specify the most specific user IDs toward the beginning of the table because the first match, rather than the best match, determines administrator authority. BMC recommends that the last entry in the list contain all asterisks for the user ID and deny administrator authority. This ensures that only the users that you specifically identify in the user ID list have authority to create and modify user access profiles.

- **RACF or an equivalent security product**
  You can use RACF or equivalent commands to define the resource and permit users to access it. Member ETAXRCN0 of the ETASAMP library contains sample statements that you can use.

  For detailed instructions for establishing administrator authority and creating user access profiles, see To establish administrator authority (see page 147) and To create user access profiles (see page 149).

To establish administrator authority

1. Determine how you want to establish administrator authority for user access profiles:
1. If you want to establish administrator authority through
   A user ID list  Go to Step 2 (see page 148)
   RACF or an equivalent security product  Go to Step 3 (see page 148)

2. Establish administrator authority through a list of user IDs.
   a. Specify the user ID and administrator authority.
      Use the $ETAUID macro instruction in member ETMXUID0 of the ETASAMP library.
      Use the following format:

      $ETAUID userid,control-flag

      The following values are valid for control-flag: Y indicates that the user ID should have administrator authority, and N indicates that the user ID should not have administrator authority.
   b. Repeat as needed to establish the required authority for the appropriate user IDs.

   Note: To ensure that only the users that you identify in the user ID list have authority to specify global options and create user access profiles, BMC recommends that the last entry in the list contain all asterisks for the user ID and deny administrator authority.

   c. To implement the user ID list, use JCL similar to that in member ETA#UIDL of the ETACNTL library to assemble and relink the panel processor module.
      If you do not use the JCL that is provided with the product to perform this step, ensure that the ETASAMP library is included in the SYSLIB concatenation for the JCL that you use.

3. Establish administrator authority through RACF or an equivalent security product.
   a. Perform one of the following actions:

      | If your facility uses         | Then                                                                 |
      |-------------------------------|----------------------------------------------------------------------|
      | RACF (any currently-supported version) | No special statements or maintenance are required. Go to Step 3.b (see page 149). |
      | ACF2 Version 1.6.0 or higher  | Add the following SAFDEF entry to your ACF2 parameters: |

      |              | FUNCRET(4) FUNCRRN(0) ID(prd)
      |              | MODE(IGNORE)
      |              | RACROUTE(REQUEST=AUTH CLASS=prd#)
      |              | RETCODE(4)

      This ensures the use of internal security (any of the available approaches). To use the SAF security interface, you must delete this SAFDEF entry.
b. Use the RACF RDEFINE command (or, for other security products, its equivalent) to define the product to class APPL. You can use RDEFINE to specify as many parameters as required. Following is an example of the RDEFINE command:

```
RDEFINE APPL ETA UACC(READ)
```

c. Use the RACF PERMIT command or equivalent to grant administrator authority to user IDs, as necessary. Following is an example of the PERMIT command:

```
PERMIT ETA CLASS(APPL) ID(userid) ACCESS(CONTROL)
```

d. Repeat steps Step 3.b (see page 149) and Step 3.c (see page 149) as needed to establish the required authority for the appropriate user IDs.

e. To implement the new RACF or equivalent security information, use JCL similar to that in member ETA#RSCL of the ETACNTL library to relink the panel processor module.

**To create user access profiles**

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing ETA from an ISPF options menu (see page 144) or through the CLIST that you created in Accessing ETA from a CLIST (see page 143). The Main Menu is displayed.
2. Type 7 in the selection field and press Enter. The Administration Menu is displayed.
3. Type 2 in the selection field and press Enter. The User Access Profiles panel is displayed.
4. Add a new user access profile:
   a. Type INSERT on the Command line and press Enter. The Insert User Access Profile pop-up window is displayed. 
   b. Type a user ID or masking pattern in the Userid or mask field. A masking pattern will allow a group of users to make the same types of changes for the IMSID that you specify in the following step.
   c. Type an IMSID or masking pattern in the IMSID/Group or mask field. A masking pattern will allow a user or group of users to use the same ETA features on multiple IMS systems. Press Enter. The User Access Profiles panel is displayed.
5. Specify which ETA features the user or users will be allowed to use. Type \textit{Y} as appropriate in the feature fields that are displayed for the inserted user ID or for other user IDs. The default value for each field is \textit{N}.

The \textit{Descriptor Edit} and \textit{TSS table Edit} security options are not associated with an IMSID for validation purposes. ETA selects all access profiles matching the user ID requesting access while ignoring the \textit{IMSID/Group} field. If any of the selected profiles specifies \textit{Y}, then access will be granted.

The \textit{CPUID Refresh} security option controls access to the ETA Product Authorization Primary Menu in the same way. However, access to the \textit{CPU-id} option on the Refresh Menu requires an IMSID or Group match. Thus, access to these menus may be dictated by different access profiles. Similar logic applies to editing and refreshing the message customization and command security tables associated with \textit{Exit/Msg/CS}.

\begin{center}
\textbf{Note}
\end{center}

To install ETA, you must have authority to specify IMSID options and perform CPUID functions. BMC recommends that you create only user access profiles for ETA administrators now.

6. To delete a user access profile, type \textit{D} in the \textit{A} field next to the applicable user ID and press Enter.
7. Press \textit{F3} to save changes to the user access profile.

\section*{Implementing a SAF interface to RACF (or equivalent) product1}

The SAF interface allows you to use RACF or an equivalent product to secure all product features.

By defining a special security class and defining resources to this class, you can activate the SAF interface and specify the product features that are secured. You can then allow use of product features by giving users READ authority for the appropriate resources. In a RACF environment, any product features that are not defined in the security class through the appropriate resource name are not secured and can be used by anyone who initiates a product session. For product features that provide edit and browse capabilities, UPDATE authority is required to access edit, for which browse capability will be assumed.

\begin{center}
\textbf{Note}
\end{center}

This approach to internal security is an alternative to the use of user access profiles (skip this task if you secure the product through user profiles).
To secure product features through the SAF interface

1. Add a product class to the RACF or equivalent class descriptor table that is identified in macro ICHERCDE.
   a. If you cannot use class ETA# because of class naming conventions at your site or because the class already exists, use the JCL in member ETA#SAF1 of the ETACNTL library to change the class name that the product expects the security product to use. Otherwise, add class ETA# to the class descriptor table.
   b. You must specify the following parameters for the class definition:

   ```
   MAXLTH=100
   FIRST=ANY
   OTHER=ANY
   ```

2. Add the product class to the RACF or equivalent class router table that is identified in macro ICHRFRTB.
3. Specify the product features that will be secured by defining the appropriate resources to the product class.

**Warning**

Under RACF, anyone who invokes a product session can use product features that you do not secure.

The following table identifies the ETA functions that you can secure. The table also provides each feature’s resource name. In the table, characters in italics are variables. For more information, see the Installation System documentation.

**ETA functions that you can secure**

<table>
<thead>
<tr>
<th>Type of option or function</th>
<th>ETA feature</th>
<th>Resource name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration options</td>
<td>Global options browse</td>
<td>GLOBAL.BROWSE</td>
</tr>
<tr>
<td></td>
<td>Global options edit</td>
<td>GLOBAL.EDIT</td>
</tr>
<tr>
<td></td>
<td>User profile security list browse</td>
<td>UPF.BROWSE</td>
</tr>
<tr>
<td></td>
<td>User profile security list edit/save</td>
<td>UPF.EDIT</td>
</tr>
<tr>
<td></td>
<td>Product authorization password entry</td>
<td>PASSWORD.EDIT</td>
</tr>
<tr>
<td></td>
<td>Product authorization password update</td>
<td>PASSWORD.REFRESH</td>
</tr>
<tr>
<td></td>
<td>Use of IMS commands from the ETA IMS Command panel</td>
<td>IMSCMD.cmd</td>
</tr>
<tr>
<td></td>
<td>Control region storage display</td>
<td>STORAGE.DISPLAY</td>
</tr>
<tr>
<td></td>
<td>Control region storage zap</td>
<td>STORAGE.ZAP</td>
</tr>
<tr>
<td>Type of option or function</td>
<td>ETA feature</td>
<td>Resource name</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Signon return code message</td>
<td>browse</td>
<td>SIGNON.MESSAGE.BROWSE</td>
</tr>
<tr>
<td>Signon return code message</td>
<td>edit</td>
<td>SIGNON.MESSAGE.EDIT</td>
</tr>
<tr>
<td>Signon return code message</td>
<td>refresh</td>
<td>iii.SIGNON.MESSAGE.REFRESH</td>
</tr>
<tr>
<td>User message browse</td>
<td></td>
<td>USER.MESSAGE.BROWSE</td>
</tr>
<tr>
<td>User message edit</td>
<td></td>
<td>USER.MESSAGE.EDIT</td>
</tr>
<tr>
<td>User message refresh</td>
<td></td>
<td>iii.USER.MESSAGE.REFRESH</td>
</tr>
<tr>
<td>Command Processing table</td>
<td>browse</td>
<td>COMMAND.TABLE.BROWSE</td>
</tr>
<tr>
<td>Command Processing table</td>
<td>edit</td>
<td>COMMAND.TABLE.EDIT</td>
</tr>
<tr>
<td>Delete command security</td>
<td>userID ACEE</td>
<td>iii.COMMAND.SECURITY.DELETE</td>
</tr>
<tr>
<td>Disconnect command security(userID)</td>
<td></td>
<td>iii.COMMAND.SECURITY.DISCONNECT</td>
</tr>
<tr>
<td>IMSID options</td>
<td>browse</td>
<td>iii.IMSID.BROWSE</td>
</tr>
<tr>
<td>IMSID options edit</td>
<td></td>
<td>iii.IMSID.EDIT</td>
</tr>
<tr>
<td>IMSID options refresh</td>
<td></td>
<td>iii.IMSID.REFRESH</td>
</tr>
<tr>
<td>Group options</td>
<td>browse</td>
<td>gggg.IMSID.BROWSE</td>
</tr>
<tr>
<td>Group options edit</td>
<td></td>
<td>gggg.IMSID.EDIT</td>
</tr>
<tr>
<td>Group options refresh</td>
<td></td>
<td>gggg.IMSID.REFRESH</td>
</tr>
<tr>
<td>IMS refresh functions</td>
<td>Default ALOT interval update</td>
<td>iii.ALOT.INTERVAL.REFRESH</td>
</tr>
<tr>
<td></td>
<td>Default ASOT interval update</td>
<td>iii.ASOT.INTERVAL.REFRESH</td>
</tr>
<tr>
<td></td>
<td>Default DLQ interval update</td>
<td>iii.DLQ.INTERVAL.REFRESH</td>
</tr>
<tr>
<td></td>
<td>Command security profiles update</td>
<td>iii.COMMAND.PROFILE.REFRESH</td>
</tr>
<tr>
<td></td>
<td>Command processing table update</td>
<td>iii.COMMAND.TABLE.REFRESH</td>
</tr>
<tr>
<td>TSS options</td>
<td>TSS table browse, test, and information display</td>
<td>TSS.BROWSE.tablename</td>
</tr>
<tr>
<td></td>
<td>TSS table edit, copy, and convert</td>
<td>TSS.EDIT.tablename</td>
</tr>
<tr>
<td></td>
<td>TSS table deletion</td>
<td>TSS.REMOVE.tablename</td>
</tr>
<tr>
<td></td>
<td>TSS table load (for more information, see the installation guide)</td>
<td>TSS.LOAD.tablename</td>
</tr>
<tr>
<td></td>
<td>TSS table unload (for more information, see the installation guide)</td>
<td>TSS.UNLOAD.tablename</td>
</tr>
<tr>
<td></td>
<td>TSS table definition</td>
<td>TSS.DEFINE.tablename</td>
</tr>
<tr>
<td></td>
<td>TSS data set format</td>
<td>TSS.FORMAT</td>
</tr>
<tr>
<td></td>
<td>TSS data set backup</td>
<td>TSS.BACKUP</td>
</tr>
</tbody>
</table>
### Type of option or function | ETA feature | Resource name
--- | --- | ---
|  | TSS data set reorganization | TSS.REORG
|  | TSS data set status | TSS.STATUS
|  | TSS data set refresh | TSS.REFRESH
| Descriptor list options | Descriptor list edit and save | DESCRIPT.EDIT.desclistname
|  | Descriptor list check | DESCRIPT.CHECK.desclistname
|  | Descriptor list execution | DESCRIPT.EXECUTE.desclistname
|  | Reload device descriptor table DFSUDT0x | DESCRIPT.RELOAD
| Exit options | Exit deactivation | EXIT.DEACT
|  | Exit reactivation | EXIT.REACT
|  | Exit reload | EXIT.RELOAD
|  | Exit status | EXIT.STATUS
| Activation of SAF security interface |  | Step 5 (see page 153)

4. Give users read authority for the resources (product features) that they need to use. For features that provide browse and edit capabilities, specify READ authority for browse and UPDATE authority for edit. Browse capability will be assumed for users with edit capability.

5. Define the ACTIVATE resource to the product class. When you define this resource, RACF or an equivalent security product restricts access to the product features that you specified, and user access profile checking is disabled.

### Setting global options in ETA

This section describes the procedures for setting global options.

Use global options to specify parameters that govern product operations throughout your site, regardless of IMS system. You must review and save the global options if you are performing an initial installation of ETA.

ETA consists of various elements that are associated through VTAM and normal IMS inter-region communication. You must specify certain parameters to keep these elements operating according to the standards at your site. Global options apply to all TSO/ISPF sessions, batch functions, BMCXLINK, and all control regions that ETA services. When you create or change global options, load module ETA$GBL1 is link-edited to your ETA options library.

⚠️ **Note**
When global options are changed, other users must re-enter ETA to obtain the revised options. For proper operation, you should recycle BMCXLINK.

To set global options

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing ETA from an ISPF options menu (see page 144) or through the CLIST that you created in Accessing ETA from a CLIST (see page 143).
   The Main Menu is displayed.
2. Type 7 in the selection field and press Enter.
   The Administration Menu is displayed.
3. Type 1 in the selection field and press Enter.
   The Global Options Entry panel is displayed.

   **Global Options Entry panel**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>prd</td>
<td>Global Options Entry</td>
<td>Command ===&gt; _________________________________________________________________</td>
</tr>
<tr>
<td>Specify the library containing the Global Options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Options library . 'prd.APF.LOAD'</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify additional libraries in which to save Options (if desired).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save library 1 . . . . .</td>
<td>Save library 2 . . . . .</td>
<td></td>
</tr>
</tbody>
</table>

4. In the **Global Options library** field, type the data set name of the library in which the global options module will reside.

   **Note**

   The ETA interface obtains the global options module from one of the following sources:
   - TSO logon procedure //STEPLIB concatenation
   - Product CLIST ISPLLILIB concatenation

5. (optional) If your installation stores the global options module in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the global options module in the **Save library 1** field and press Enter.

   **Note**
If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

The Edit Global Options panel is displayed.

**Edit Global Options panel**

The following fields are available on this panel:

**VTAM User Session ACBNAME prefix**
Specify the four-character ACBNAME prefix from the VTAM definition statements that were created during the product installation.

The BMCXLINK ACBNAMEs that are used in the VTAM definition statements must be of the format `ppppnnnn`, where `pppp` is the four-character prefix specified in this field, and `nnnn` is the next available sequential number starting with 0001.

The default value for this field is ETMU.

**DASD unit name for temporary files**
Specify the esoteric DASD unit name that the product Log and History File functions use to allocate work files and temporary report files during sorts.

The default value for this field is `SYSALLDA`.

**Trace table dynamic dump sysout class**
Specify the sysout class to be used if the internal trace table appears in any abend dumps.

This class is also used if the table must be printed on demand.

The default value for this field is `A`.

**Request status check time interval**
Specify the time interval, in seconds, after which ETA will provide a status on any outstanding requests. ETA periodically responds to the BMCXLINK user session while processing a request for that session so that the user stays informed of the request processing status.

The default value for this field is 10 seconds.

**Routing code**

Type the WTO message routing code that ETA and BMCXLINK will use. BMCXLINK issues WTO messages any time significant events occur. Use the WTO routing code to direct these messages to selected consoles.

BMC recommends that you use the default value of 11.

For information about other routing codes, see IBM publication MVS/ESA Routing and Descriptor Codes or z/OS MVS System Messages.

**Descriptor code**

Type the WTO message descriptor code that ETA and BMCXLINK will use. BMCXLINK issues WTO messages any time significant events occur. You can suppress these messages depending on the WTO message descriptor code specified.

BMC recommends that you use the default value of 7.

For information about other descriptor codes, see IBM publication MVS/ESA Routing and Descriptor Codes or z/OS MVS System Messages.

**Translate all messages to uppercase**

Type a 1 in the selection field to translate product-generated messages to uppercase. Otherwise, messages are generated in mixed case.

This option affects only the messages that are displayed on the console or in batch. It does not affect ISPF messages unless the message comes from BMCXLINK.

**Message number prefix**

Select a message prefix.

Type 1 in the selection field to prefix the error message with the BMCETA prefix (for example, BMCETA123456E).

Type 2 in the selection field to prefix the error message with the ETA prefix (for example, ETA123456E).

Type 3 in the selection field to prefix the error message with the BMC prefix (for example, BMC123456E).

6. **User Profiles data set**

Specify the name of the data set that will store the user access profiles that provide internal product security. This data set is allocated during initial installation.

7. Press F3 to save changes to the global options.

## Setting IMSID options for ETA

This section describes the procedures for setting IMSID options.

You should set IMSID options if you are performing an initial installation of ETA.
For ETA to access an IMS system, you must define the system to ETA with a set of IMSID options. When you create or change IMSID options, the load module ETA#iii (where iii is the IMSID) is link-edited to your ETA options library.

You must create IMSID basic options for each control region that ETA services. For more information, see To set IMSID options (see page 157).

You can also set TSS options for the IMSID. For more information, see Setting TSS IMSID options (see page 160).

**Note**

BMC recommends the following regarding the IMSID options modules:

- Use the APF-authorized library to provide both ISPF and IMS with access to the IMSID options modules.
- Do not use a LINKLIST library to store the IMSID options modules
- Save IMSID options modules in the same library with the global and Group options (if used) modules.

To set IMSID options

**Note**

The IMSID options module that you will create in this task will contain only the information that is required to start ETA. For full information about using ETA to set IMSID options, see the EXTENDED TERMINAL ASSIST PLUS User Guide.

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing ETA from an ISPF options menu (see page 144) or through the CLIST that you created in Accessing ETA from a CLIST (see page 143). The Main Menu is displayed.
2. Type 1 in the selection field and press Enter. The IMSID/Group Options Entry panel is displayed.

**IMSID/Group Options Entry panel**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETA</td>
<td>IMSID/Group Options Entry</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>

---
3. Type 1 in the selection field.
4. Type the data set name of the library in which the IMSID options module (ETA#iii) will reside in the **Options library** field.
5. Perform the appropriate action.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicate a specific IMSID for the IMS system that you want to customize or access.</td>
<td>Type the IMSID of the IMS system in the <strong>IMSID or Group</strong> field. This action is required for the first set of IMSID options.</td>
</tr>
<tr>
<td>Choose an IMSID that you want to customize or access from a list of IMSIDs.</td>
<td>Leave the <strong>IMSID or Group</strong> field blank.</td>
</tr>
</tbody>
</table>

6. (optional) If your installation stores IMSID/Group options modules in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the IMSID options modules in the **Save library 1** field and press Enter.

**Note**

If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

If you typed a specific IMSID in the IMSID or Group field, the Edit IMSID Options panel is displayed. Go to [Step 8](see page 159).
If you left the IMSID or Group field blank, the Edit IMSID Options - List panel is displayed, allowing you to select an IMSID. Go to [Step 7](see page 159).

**Edit IMSID Options - List panel**

<table>
<thead>
<tr>
<th>Command</th>
<th>Options Library . . : 'ABC.prd.OPTIONS.LOAD'</th>
</tr>
</thead>
<tbody>
<tr>
<td>prd</td>
<td>Edit IMSID Options - List</td>
</tr>
</tbody>
</table>
Enter S to edit the IMSID options.

- ABCD
- BAD1
- GCB5
- MJD5
- NEW
- PXMI
- TEST
- WXCA

7. Perform one of the following actions:
   - Create a new IMSID options module by typing S newimsid on the Command line.
   - Modify an existing set of options by typing S next to an existing IMSID.

Press Enter.

The ETA Edit IMSID Options panel is displayed.

8. Type 1 in the selection field and press Enter.

The IMSID Options – Basic Options panel is displayed.

The following fields are available on this panel:

**IMSID**

The IMSID of the options module that you selected.

**IMS version/release level**

Type the IMS version and release for the IMSID. Possible values are:

- IMS Version 13.1
- IMS Version 14.1
- IMS Version 15.1

You can specify an IMS level for each IMS system that uses ETA. The product can support a combination of IMS systems.

**Allow IMS storage displays**

Type a / in the selection field to enable the storage display feature for this IMS system. You can use internal security to restrict usage of this feature.

**Allow IMS storage zaps**

Type a / in the selection field to enable the storage alteration (zap) feature for this IMS system.

The storage zap feature is a powerful tool for correcting problems within the IMS system. However, you should use internal security to restrict usage of this feature.

**Copy IMSID options to an IMS STEPLIB library when saved**

Type a / in the selection field to copy IMSID options modules to an IMS //STEPLIB library when the module is saved in the options library.

If you select this option, you must specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region in the IMS STEPLIB library field.

**IMS STEPLIB library**

Specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region.
If your installation stores IMSID options modules in separate libraries for use by ISPF and IMS, you should complete this field. If both ISPF and IMS use the same library, this field is optional.

**XRF/FDR Alternate IMSID**
Specify the IMSID of the IMSGEN-defined XRF alternate system or the IMSID of the FDR control region.

**XCF Group**
Specify the name of the Group to which this IMS system belongs. This field is optional because an IMS system does not have to belong to a Group.

**BMCXLINK task network LUNAME**
Type a network LUNAME for the BMCXLINK VTAM subtask. The LUNAME that you specify MUST match the LUNAME that is specified in the PARM field of the BMCXLINK task. The default value for this field is ETAALINK.

9. Press F3 to save changes to the IMSID options.
   - If you specified an existing IMSID in the **XRF/FDR Alternate IMSID** field, the Confirm Delete pop-up window is displayed before the IMSID options are saved.
   - Type 1 in selection field and press Enter to delete the existing options for the IMSID previously specified in the **XRF/FDR Alternate IMSID** field. This selection also makes the IMSID that is specified in the **XRF/FDR Alternate IMSID** field the alternate for the IMSID that you are editing.

## Setting TSS IMSID options

If you plan to use the ETA Translate Sub-system (TSS) feature, you must specify TSS information.

To specify TSS information for ETA, perform the following steps:

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing ETA from an ISPF options menu (see page 144) or through the CLIST Accessing ETA from an ISPF options menu (see page 143) that you created in Accessing ETA from a CLIST (see page 143). The Main Menu is displayed.
2. Type 5 in the selection field and press Enter. The IMSID/Group Options Entry panel is displayed.
3. Type 1 in the selection field.
4. Type the data set name of the library in which the ETA IMSID options module (ETA#iii, where iii is the IMSID) resides in the Options library field.
5. (optional) If your installation stores ETA IMSID/Group options modules in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the IMSID options modules in the Save library 1 field. If ISPF, IMS, and BMCXLINK use the same library, this field is optional.

⚠️ Note

If your installation stores IMSID options modules in separate libraries for use by ISPF and IMS, you should complete this field. If both ISPF and IMS use the same library, this field is optional.
If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

Press **Enter**.
The Edit IMSID Options – List panel is displayed, allowing you to select an IMSID.

6. Type **S** next to the IMSID that you want to customize or access and press **Enter**.
The Edit IMSID Options panel is displayed.

7. Type **2** in the selection field and press **Enter**.
The IMSID Options – TSS Options panel is displayed.
The following fields are available on the IMSID Options – TSS Options panel:

   **IMSID**
The IMSID of the options module that you selected.
This is not an editable field.

   **TSS table data set name**
The name of the TSS data set.

**Note**
The TSS data set must already be allocated. For information about allocating the TSS data set, see the *EXTENDED TERMINAL ASSIST PLUS User Guide*.

**Number of cache buffers**
The number of TSS cache buffers that ETA will allocate for TSS use.

**Note**
For best performance, the number of buffers should equal the sum of the number of index and table blocks plus one buffer for the control record. Table blocks can be obtained from the Table Select panel (ETMATS), and index blocks can be obtained from TSS option 13, Status of TSS data set.

**RCNT TSS table name**
The name of a TSS table that contains MSNAME information for the creation of dynamic remote LTERMs.

**Assume ALLROWS keyword on /DIS TSSTABLE command**
A *I* indicates that the ALLROWS keyword will be assumed on the /DIS TSSTABLE command.
To prevent the /DIS TSSTABLE command from automatically displaying a list of all rows in the specified TSS table, do not select this option. When this option is deactivated, users must issue the /DIS TSSTABLE tablename ALLROWS command to display a list of all rows in the specified TSS table.
If you have large TSS tables and do not want users to fill message queues and consume system resources by accidentally displaying all rows in the TSS tables, BMC recommends that you do not select this option.

8. Edit the fields as necessary.
9. Save the changes to the TSS information.

Setting Group options for ETA

This section describes the procedures for setting Group options.

Group options allow you to treat a user-defined group of IMS systems as one IMS system. A group of IMS systems would typically be an IMS Datasharing Group, IMS Shared Queues Group, or a group of logically related or duplicated IMS systems. When you create or change Group options, the load module ETAZgxxx is link-edited to your options library.

⚠️ Note

Group options are NOT required.

Once you have saved the Group options module, you will have to restart IMS for the changes to take effect. If you perform a Group options REFRESH, the only changes that will take effect are the IMS command options.

⚠️ Note

When you are choosing a name for your Group options, be sure that you do not duplicate the name used for existing IMSID options. If you duplicate the IMSID options name for your Group options name, the product will not find the Group options because it will locate the IMSID options first.

BMC recommends the following regarding the Group options module:

- Use the APF-authorized library to provide both ISPF and IMS with access to the Group options module.
- Do not use a LINKLIST library to store the Group options module.
- Save the Group options module in the same library with the global and IMSID options modules.
To set Group options

1. Invoke the online interface through the modified ISPF/PDF Primary Option Menu that you created in Accessing ETA from an ISPF options menu (see page 144) or through the CLIST that you created in Accessing ETA from a CLIST (see page 143). The Main Menu is displayed.
2. Type 5 in the selection field and press Enter.
   The IMSID/Group Options Entry panel is displayed.
3. Type 2 in the selection field.
4. Type the data set name of the library in which the Group options module (ETAZgggg) resides in the Options library field.
5. Perform the appropriate action:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicate a specific Group that you want to customize or access.</td>
<td>Type the name of the Group in the IMSID or Group field.</td>
</tr>
<tr>
<td>Choose a Group that you want to customize or access from a list of Groups.</td>
<td>Leave the IMSID or Group field blank.</td>
</tr>
</tbody>
</table>

6. (optional) If your installation stores IMSID/Group options modules in separate libraries that are used by ISPF, the control region, or BMCXLINK, type the data set name of the additional library in which to store the Group options modules in the Save library 1 field. If ISPF, the control region, and BMCXLINK use the same library, this field is optional.

⚠️ **Note**

If you use several load libraries, remember that it is possible to have a copy of a module in more than one library. IMS will use the first module that it finds, regardless of whether that module is the most current one available.

Press Enter.

<table>
<thead>
<tr>
<th>Previous action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>You typed a specific Group name in the IMSID or Group field.</td>
<td>The Edit Group Options panel is displayed. Go to Step 8 (see page 163).</td>
</tr>
<tr>
<td>You left the IMSID or Group field blank.</td>
<td>The Edit Group Options - List panel is displayed so that you can select a group. Go to Step 7 (see page 163).</td>
</tr>
</tbody>
</table>

7. Type S next to the Group that you want to customize or access and press Enter.
   The Edit Group Options panel is displayed.
8. Specify the Group options.
   The following fields are available on this panel:

   **Group name**
The name of the Group that you are creating or modifying. This is not an editable field.

**BMCXLINK task network LUNAME**

Type a network LUNAME for the BMCXLINK VTAM subtask. The LUNAME that you specify MUST match the LUNAME that is specified in the PARM field of the BMCXLINK task.

The default value for this field is **BMCALINK**.

**Copy Group Options to an IMS STEPLIB library when saved**

Type a / in the selection field to copy Group options modules to an IMS //STEPLIB library when the module is saved in the options library.

If you select this field, you must specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region in the IMS STEPLIB library field.

**(optional) IMS STEPLIB library**

Specify the name of the IMS //STEPLIB library in which to store the modules that are used by the control region.

Use this field if your installation stores Group options modules in separate libraries for use by ISPF and IMS. If both ISPF and IMS use the same library.

9. Press F3 to save changes to the Group options.

---

**Starting ETA**

You must start ETA after you complete the other configuration tasks that are described in this section (see page 138).

1. Verify that the IMSID options module (ETA#iii) and the product authorization module (ETATBL3P for a permanent password or ETATBL3T for a temporary password) are stored in an APF-authorized library.

2. Verify the parameters in the IMS control region JCL and in PROCLIB member DFSPBxxx, if applicable.
   a. Verify that PROCLIB member DFSPBxxx contains the statement ETO=Y. ETO must be active for ETA to function.
   b. Perform any of the following actions:

<table>
<thead>
<tr>
<th>If you...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>want to allow multiple signons per userID</td>
<td>verify that the value that is specified for the SGN parameter is G or Z.</td>
</tr>
<tr>
<td>do not need multiple signons per userID</td>
<td>go to Step 5 (see page 164).</td>
</tr>
</tbody>
</table>

3. Specify the ISPF options library name in the BMCXLINK started task JCL.
   Member ETA#LINK of ETACNTL provides sample JCL for BMCXLINK.

4. Start the BMCXLINK job (or started task) on each CPU where an IMS control region that is serviced by ETA will run.
   For information on commands that you can issue for BMCXLINK, issue the HELP command against the BMCXLINK outstanding reply.

5. Warm-start IMS.
6. Repeat this task for other IMSIDs if necessary, starting with Step 2 (see page 164).

**Customizing LOCAL COPY PLUS**

This section describes customization tasks that are unique to the LOCAL COPY PLUS product. *Customization* refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered in this section:

- Overview of customizing Local Copy Plus (see page 165)
- LOCAL COPY PLUS customization worksheet (see page 166)
- Adding LOCAL COPY PLUS to TSO/ISPF (see page 166)
- Limiting access to LOCAL COPY PLUS (see page 172)
- Setting LOCAL COPY PLUS options (see page 177)

**Overview of customizing Local Copy Plus**

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and configuring the product libraries, see the Installation System documentation.

⚠️ **Note**

No configuration tasks were performed for LOCAL COPY PLUS.

The customization tasks that are presented are unique to LOCAL COPY PLUS.

Use the following general guidelines when you set the LOCAL COPY PLUS options:

- You can replace LCPTRAN1 with the name of your choice.
  If you change the name, ensure that you also change it in the LOCAL COPY PLUS options and that you update all references in LCPCNTL members LCPMFS22 and LCPMFS32.
- If you specify a SEGSIZE value, it must be at least 2048 bytes.
- If you specify a SEGNO value, it must be 50 or more. If you use Routing Lists, SEGNO should be set to zero.
- For the transaction to function properly, you should define it as `response mode`. You should define terminals that use the system administrator panels as TRANRESP in the IMSGEN.
- LCPTRAN1 should not be pre-loaded.
- If you are operating in a shared queues environment (CQS) and you want to ensure that LCPTRAN1 runs on the originating system, specify SERIAL=YES.
LOCAL COPY PLUS customization worksheet

Refer to the following worksheet as you work through the customization process for LOCAL COPY PLUS:

<table>
<thead>
<tr>
<th>Done</th>
<th>Step</th>
<th>Page</th>
</tr>
</thead>
</table>
|      | 1. Provide access to the ISPF interface through a CLIST or through an ISPF options menu. | • Adding LOCAL COPY PLUS to TSO/ISPF (see page 166)  
• Accessing LOCAL COPY PLUS from a CLIST (see page 167)  
• Accessing LOCAL COPY PLUS from an ISPF options menu (see page 167)  
• Setting LOCAL COPY PLUS default ISPF IMSID values (see page 170)  
• Setting LOCAL COPY PLUS default ISPF IMSID values (see page 170) |
|      | 2. Limit access to LOCAL COPY PLUS through an internally coded list, ACF2, or RACF. | • Limiting access to LOCAL COPY PLUS (see page 172)  
• Implementing an internally coded list (see page 173)  
• Implementing ACF2 (see page 175)  
• Implementing RACF (see page 176) |
|      | 3. Set LOCAL COPY PLUS options.                                        | • Setting LOCAL COPY PLUS IMSID options (see page 177)  
• Setting LOCAL COPY PLUS IMSID options (see page 177)  
• Specifying LOCAL COPY PLUS Destination Entries (see page 178)  
• Setting LOCAL COPY PLUS Copy Table Entry options (see page 178) |

Adding LOCAL COPY PLUS to TSO/ISPF

This section describes the procedures for adding LOCAL COPY PLUS to TSO/ISPF.

You can install the online interface so that you can invoke it from a CLIST or from an ISPF options menu. For more information, see Accessing LOCAL COPY PLUS from a CLIST (see page 167) and Accessing LOCAL COPY PLUS from an ISPF options menu (see page 167)
Accessing LOCAL COPY PLUS from a CLIST

A sample CLIST that provides access to the online interface using LIBDEF is available in the SAMP library. You can copy member LCPCI@00 of the SAMP library into your CLIST library and update the following data set names to reference your data sets:

- &LCPLIB
- &LCPMLIB
- &LCPPLIB

Accessing LOCAL COPY PLUS from an ISPF options menu

Accessing LOCAL COPY PLUS from an ISPF options menu requires that you pre-allocate the necessary ISPF data sets to the user.

You must add the following libraries to the TSO logon procedure for each user who requires access to LOCAL COPY PLUS:

- Load library (ISPLLIB)
- Panel library (ISPPLIB)
- Message library (ISPMLIB)

Note

There are additional tasks related to accessing LOCAL COPY PLUS from an ISPF options menu. For more information, see Setting LOCAL COPY PLUS default ISPF values (see page 168) and Setting LOCAL COPY PLUS default ISPF IMSID values (see page 170).

The following figure shows a sample ISPF/PDF Primary Option Menu that has been modified to access LOCAL COPY PLUS.

Sample modifications to ISPF/PDF Primary Option Menu

```markdown
%-----------------------  ISPF/PDF PRIMARY OPTION MENU  ------------------
%OPTION  ===>                                                           +
%  0  +ISPF PARMS  - Specify terminal and user parameters
%  1  +BROWSE      - Display source data or output listings
%  2  +EDIT        - Create or change source data
%  3  +UTILITIES   - Perform utility functions
%  4  +FOREGROUND  - Invoke language processors in foreground
%  5  +BATCH       - Submit job for language processing
%  6  +COMMAND     - Enter TSO command or CLIST
%  7  +DIALOG TEST - Perform dialog testing
```
Setting LOCAL COPY PLUS default ISPF values

After you install the TSO/ISPF panel and messages members for LOCAL COPY PLUS, you may want to review and modify the default ISPF values for the variables that the product uses (listed in the following table).

You can set values for the variables in panel LCPPS@00.

LOCAL COPY PLUS variables
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;LCP2ALM</td>
<td>A YES or NO value used as the operand of the ALARM control word in all LOCAL COPY PLUS ISPF message definitions</td>
</tr>
<tr>
<td>&amp;LCP2DFMT</td>
<td>An eight-character user date format code that defaults to mm/dd/yy in order to display LOCAL COPY PLUS dates according to internal BMC conventions</td>
</tr>
<tr>
<td></td>
<td>You can change the order of mm, dd, and yy as long as all three symbols appear exactly once in the same set of columns (e.g., column 1, column 4, and column 7). You can replace columns 3 and 6 (the slashes above, '/') with any other appropriate characters that aid the readability of the date (e.g., yy-mm-dd would format June 22nd, 1988 as 88-06-22).</td>
</tr>
<tr>
<td>&amp;LCP2IMD</td>
<td>A four-character default IMSID value</td>
</tr>
<tr>
<td>&amp;LCP2CRV</td>
<td>The six-character default Copy Table recovery data set volume serial to be used when allocating the recovery data set while editing a LOCAL COPY PLUS Copy Table</td>
</tr>
<tr>
<td>&amp;LCP2CRU</td>
<td>The eight-character default Copy Table recovery data set unit name to be used when allocating the recovery data set while editing a LOCAL COPY PLUS Copy Table</td>
</tr>
<tr>
<td>&amp;LCP2EDV</td>
<td>A six-character default ISPF edit work file volume serial to be used under ISPF 2.2 and earlier to allocate a temporary work file for editing LOCAL COPY PLUS News Members</td>
</tr>
<tr>
<td>&amp;LCP2EDU</td>
<td>The eight-character default ISPF edit work file unit name to be used under ISPF 2.2 and earlier to allocate a temporary work file for editing LOCAL COPY PLUS News Members</td>
</tr>
<tr>
<td>&amp;LCP2EDI</td>
<td>The eight-character ISPF release level constant</td>
</tr>
<tr>
<td></td>
<td>You should not modify this value unless directed BMC for debugging purposes.</td>
</tr>
<tr>
<td>&amp;LCP2VOL</td>
<td>The six-character default ISPF table library volume serial to be used when creating a new shared &amp;LCP. IMSID list</td>
</tr>
<tr>
<td>&amp;LCP2UNT</td>
<td>The eight-character default ISPF table library unit name to be used when creating a new shared &amp;LCP. IMSID list</td>
</tr>
<tr>
<td>&amp;LCP2ZTB</td>
<td>The eight-character ISPF table name which will contain the list of IMSIDs to be displayed on the &amp;LCP. Primary Menu</td>
</tr>
<tr>
<td></td>
<td>If the ISPF table does not previously exist, &amp;LCP. will automatically create a new ISPF table with one IMSID (the IMSID specified by &amp;LCP2IMD above).</td>
</tr>
<tr>
<td>&amp;LCP2LIB</td>
<td>The 44-character partitioned data set name of the ISPF table library to be used to save the list of IMSIDs to be displayed on the &amp;LCP. Primary Menu</td>
</tr>
<tr>
<td></td>
<td>Using this data set name, &amp;LCP. will try to find the ISPF table specified by &amp;LCP2ZTB above, or will automatically create a new ISPF table library data set (e.g., like the IBM data sets allocated to ISPTLIB) if it does not already exist (see the ISPF and ISPF/PDF Installation and Customization manual for ISPF table data set DCB information).</td>
</tr>
</tbody>
</table>

If you want to modify any of the variables, edit the source for ISPF panel LCPPS@00 in LCPPLIB. Change the )INIT section before any other LOCAL COPY PLUS ISPF users have a chance to use the ISPF panels. Once an individual uses the ISPF panels, some of the above variables are stored in their ISPF profile and cannot be reset by a simple execution of the LCPPS@00 panel (most notably, the &LCP2LIB and the &LCP2IMD variables).
Pay particular attention to the &LCP2VOL, &LCP2UNT, and &LCP2LIB variables, as the associated values will be used to dynamically create an ISPF table library if it does not already exist. As an optional preparation step, you can pre-allocate this library (using the standard ISPF DCB characteristics for table libraries). However, you must then specify the pre-allocated partitioned data set name as the value for the &LCP2LIB variable.

Other important variables to review are the copy-table recovery and edit work-file UNIT/VOLSER variables. You should define the copy-recovery unit/volser variables so that short-term, permanent TSO data sets can be allocated under the then active userid. You should define the edit work-file unit/volser variables so that an MVS temporary data set can be allocated, used, and deleted during a LOCAL COPY PLUS news member edit session (for ISPF 2.3 and later, the EDIF service is used in place of EDIT, so these two variables are ignored).

The INIT section of ISPF panel LCPPS@00 contains several important default data set specifications.

**ISPF profile defaults for LOCAL COPY PLUS**

```
/* -------------------------------- */
/* --- USER-MODIFIABLE DEFAULTS --- */
&LCP2ALM = YES                      /* <== SET YES/NO FOR .ALARM=YES/NO */
&LCP2DFMT = 'MM/DD/YY'              /* <== SET USER DATE-FORMAT:
    (DD/MM/YY, YY-MM-DD, ETC.)
    */
IF (&LCP2IMD = &Z)                  /*<== VERIFY DEFAULT IMSID */
    &LCP2IMD = 'IMSA'                      /*<== VERIFY DEFAULT IMSID */
    /*
    &LCP2CRV = &Z                       /*<== VERIFY COPY-RECOVERY VOL */
    &LCP2CRU = 'SYSDA'                  /*<== VERIFY COPY-RECOVERY UNIT */
    /*
    &LCP2EDV = &Z                       /*<== VERIFY EDIT WORK FILE VOL */
    &LCP2EDU = 'SYSDA'                  /*<== VERIFY EDIT WORK FILE UNIT */
    &LCP2EDI = TRUNC (&ZENVIR,8)        /*<== VERIFY LCP/ISPF ENVIRONMENT */
    /*
    &LCP2VOL = &Z                       /*<== VERIFY IMSID TABLE LIB VOL */
    &LCP2UNT = 'SYSDA'                  /*<== VERIFY IMSID TABLE LIB UNIT */
    &LCP2ZTB = 'LCP2IMSL'               /*<== VERIFY IMSID TABLE NAME */
    /*
    &LCP2LIB = 'BMCNODE.LCPTLIB'        /*<== VERIFY IMSID TABLE LIBRARY */
/*
```

Within the limits of ISPF panel syntax, you can modify the assignment statements to suit the environment at your site.

Once you have updated your logon procedure (proc), log off ISPF and log back on.

**Setting LOCAL COPY PLUS default ISPF IMSID values**

After you modify the ISPF environmental default values, you should also review the ISPF IMSID default values.
If you plan to have LOCAL COPY PLUS manage more than one or two IMSIDs, you should preset appropriate default values for the IMSID options.

**Note**

For information about modifying the ISPF environmental default values for LOCAL COPY PLUS, see Setting LOCAL COPY PLUS default ISPF values (see page 168).

The following table lists ISPF IMSID variables that you might want to modify.

### LOCAL COPY PLUS ISPF IMSID variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;LCPGPFKN</td>
<td>The two-character PF key number to be used when requesting COPY processing</td>
</tr>
<tr>
<td>&amp;LCPGXCTN</td>
<td>The eight-character IMS/VS name of the transaction that processes LOCAL COPY PLUS panel copy requests</td>
</tr>
<tr>
<td>&amp;LCPGRESL</td>
<td>The 44-character data set name of the IMS/VS resident library where the IMS/VS SYSTEM modules and the control region portion of the LOCAL COPY PLUS modules reside</td>
</tr>
<tr>
<td>&amp;LCPGLPDX</td>
<td>The 44-character data set name of the LOCAL COPY PLUS PDX data set where the Copy Table and destination information will be stored</td>
</tr>
</tbody>
</table>

The following figure shows the PROC section of ISPF panel LCPPS@01, where the ISPF IMSID variables are defined.

### ISPF IMSID defaults in panel LCPPS@01

```
&LCPGPFKN = '12'                   /* PF KEY FOR SCREEN COPY        */
&LCPGTBLS = '00'                   /* ACTIVE COPY TABLE SUFFIX      */
&LCPGXLTN = 'LCPTRAN1'             /* XCTN FOR ADMIN. FUNCTIONS     */
&LCPGXCTN = 'LCPTRAN1'             /* XCTN TO REQUEST SCREEN COPY   */
&LCPGCDTE = '&ZDATE'               /* ORIGINAL CREATION DATE        */
&LCPGMTME = '&ZTIME'               /* ORIGINAL CREATION TIME        */
&LCPGMDTE = '00/00/00'             /* LAST-MODIFIED DATE            */
&LCPGMTME = '00:00'                /* LAST-MODIFIED TIME            */
&LCPGMUSR = '&ZUSER'               /* LAST-MODIFYING USERID         */
&LCPGRESL = 'LCP.V2.LOAD'          /* IMS/VS RESIDENT LIBRARY       */
&LCPGLPDX = 'LCP.V2.&LCP2IMD..PDX' /* LCP/PDX LIBRARY NAME          */
&LCPGUNIT = 'SYSDA'                /* LCP/PDX UNIT-NAME             */
&LCPGVLSR = ' '                    /* LCP/PDX VOLUME-SERIAL         */
&LCPGFORM = 'STD '                 /* JES FORMS CODE                */
&LCPGMFSF = 'LC'                   /* LCP/MFS MOD NAME PREFIX       */
&LCPGSOUT = 'A'                    /* JES SYSOUT CLASS              */
&LCPGCPYT = 'L'                    /* COPY-ENTRIES ASSIGNED BY L/P/U */
&LCPGNODE = 'N1 '                  /* JES NODE FOR VM/CMS DESTS     */
&LCPGSMFL = ' '                    /* SIGNON FORMAT NAME (DFS2002)  */
&LCPGSMFM = ' '                    /* APPLCTN MENU FMT NAME (DFS058)*/
&LCPGDCNT = ' '                    /* DFLT Control-GROUP NAME       */
```
Within the limits of ISPF panel syntax, you can modify any of the processing statements in panel LCPPS@01 to suit your installation environment.

## Limiting access to LOCAL COPY PLUS

This section describes the procedures for limiting access to LOCAL COPY PLUS.

By default, access to many product functions is unlimited. To restrict product usage, you must take steps to protect the functions that you want to restrict.
Under most circumstances, you do not have to set security when initially installing LOCAL COPY PLUS. Therefore, you may want to defer setting security until you have reviewed the various security methods.

LOCAL COPY PLUS allows you to secure product features through the following methods:

- Internally coded list
  For more information about implementing security through an internally coded list, see Implementing an internally coded list (see page 173).
- ACF2
  For more information about using ACF2 to secure LOCAL COPY PLUS features, see Implementing ACF2 (see page 175).
- RACF
  For more information about using RACF to secure LOCAL COPY PLUS features, see Implementing RACF (see page 176).

Implementing an internally coded list

You can use an internally coded list of function,userid,imsid authorization entries to control access to the product functions.

The default is to allow any user to access any function with any IMSID through a masked authorization entry.

The following table identifies the LOCAL COPY PLUS functions that you can secure:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTS</td>
<td>Creates and modifies IMSID-related options</td>
</tr>
<tr>
<td>DESTS</td>
<td>Creates and modifies destination entries</td>
</tr>
<tr>
<td>COPIES</td>
<td>Creates and modifies Copy Tables and Copy Table Entries</td>
</tr>
<tr>
<td>GRPS</td>
<td>Creates and modifies control-groups</td>
</tr>
<tr>
<td>NEWS</td>
<td>Creates and edits news members</td>
</tr>
<tr>
<td>ROUTS</td>
<td>Creates and modifies route-lists</td>
</tr>
<tr>
<td>UTILS</td>
<td>Executes the PDX and CPU ID utilities</td>
</tr>
<tr>
<td>IMSID</td>
<td>Inserts or deletes IMSID entries</td>
</tr>
<tr>
<td>LCP2</td>
<td>Provides general access to ISPF panels</td>
</tr>
</tbody>
</table>

To limit access to product functions through an internally coded list

1. Code the function,userid,imsid entries of the ASM source member (LCPXSMA0) of the LCPSAMP library to enable or deny access.
The ASM source member provides the interface to the internally coded list.

⚠️ Note

You can use an asterisk (*) as a wildcard character to include masking entries in the authorization list.

Use the $AUID macro instruction to specify an authorization entry as follows:

```
$AUID function,userid,imsid,access-flag
```

The following table describes the terms that are specified in the authorization entry:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>function</td>
<td>One of the protected functions that are listed in here (see page 173)</td>
</tr>
<tr>
<td></td>
<td>Use an asterisk (*) to indicate all functions.</td>
</tr>
<tr>
<td>userid</td>
<td>A specific userID or userID mask</td>
</tr>
<tr>
<td></td>
<td>The valid range is from one to eight characters. Use an asterisk (*) to</td>
</tr>
<tr>
<td></td>
<td>indicate all userIDs.</td>
</tr>
<tr>
<td>imsid</td>
<td>A specific IMSID that has been defined through IMS options specification or</td>
</tr>
<tr>
<td></td>
<td>an IMSID mask</td>
</tr>
<tr>
<td></td>
<td>The valid range is from one to four characters. Use an asterisk (*) to</td>
</tr>
<tr>
<td></td>
<td>indicate all IMSIDs.</td>
</tr>
<tr>
<td>access-flag</td>
<td>Y or N depending on whether the user can access the function with the</td>
</tr>
<tr>
<td></td>
<td>specified IMSID</td>
</tr>
</tbody>
</table>

Include as many $AUID entries as necessary in the appropriate portion of the source member LCPXSMA0. Review the default example entries and remove those that are inappropriate for your security requirements.

The authorization process searches the table from top to bottom and left to right. The first match determines the authorization. Generalized authorizations at the top or left of the list will nullify specific authorizations at the bottom or right of the list. You should place specific entries before general entries. For example, you might want to limit access for USERABC so that he can perform all functions, but only with the IMSID IMST. At the same time, you may want to let all other users access all other functions.

2. Code the $AUID macros as shown in the following figure:

```
$AUID *,USERABC,IMST,Y
$AUID *,USERABC,*,N
$AUID *,*,*,N

The entries perform the following functions:

- The first entry enables USERABC to access all product functions with the IMSID IMST.
- The second entry prohibits USERABC from accessing any product functions with any other IMSID.
```
● The third entry enables all other users to access all other functions with all other IMSIDs.

3. Use JCL similar to that provided in LCP CNTL member LCP#SMA0 to assemble the authorization entries and implement the internally-coded security authorization list. If you attempt to perform a function that is specified in an authorization entry, the product scans the internally coded list. If the product does not find a match or if the matched entry denies access, you cannot perform the function or make changes.

Implementing ACF2

You can protect LOCAL COPY PLUS functions by using ACF2 generalized resource rules to grant ISPF users limited (or unlimited) access to the functions.

To implement ACF2 control, use JCL similar to what is provided in member LCP#SMA1 in the LCPCNTL library to assemble the ACF2 interface and relink the primary LOCAL COPY PLUS panel processor module.

Before allowing ISPF users to perform product functions, LOCAL COPY PLUS issues an ACF2 Generalized Resource validation call. If the resource rule is coded to PREVENT access or if ACF2 installation exits deny access, the user cannot perform the function or cannot make updates.

Member LCPXSMA1 in the LCPCNTL library provides the interface to ACF2 services and validates a generalized resource name. The generalized resource name is created as follows:

- **R** – the class code required by ACF2 for generalized resource rules.
- **BMC** – the resource type code selected by BMC for LOCAL COPY PLUS generalized resource rules.
- **BMCLCP20** – a fixed resource name prefix selected by BMC for LOCAL COPY PLUS resource validation.
- **function** – the first character of the LOCAL COPY PLUS function to be validated.
- **imsid** – the one- to four-character active IMSID to be validated.

**Note**

When the function character is L (for example, for general access to the LOCAL COPY PLUS ISPF panels), the IMSID will always be set to CP2@.

If an ISPF user attempts to access a LOCAL COPY PLUS Route List for the IMSID IMSP, an ACF2 validation call is made for the full resource name:

```
R BMC BMCLCP20-RIMSP
```
Consider the following points regarding ACF2 resource rules:

- To create at least two ACF2 resource rules and define who may access LOCAL COPY PLUS features and facilities, use the standard ACF2 commands.
- To control who has access to the LOCAL COPY PLUS ISPF panels, use the full resource name, R BMC BMCLCP20-LCP2@.
- To control accesses to the individual functions by IMSID, by function, and by userid, use individual or masking ACF2 resource rules.
- To use resource name masking, ACF2 generalized resource rules for the type code, BMC, must be resident.

For example, to use ACF2 resource name masking to control all types of individual access to IMSID IMST in one AFC2 rule set, you could use the following resource name:

```
R BMC BMCLCP20-*IMST
```

## Implementing RACF

You can control access to LOCAL COPY PLUS functions by using a RACF-protected resource to grant individual users access to the functions.

To implement RACF control, use JCL similar to what is provided in member LCP#SMA2 in the LCPCNTL data set to assemble the RACF interface and relink the primary LOCAL COPY PLUS panel processor module.

Before allowing an ISPF user to perform functions, LOCAL COPY PLUS issues an RACHECK macro instruction. If the RACHECK macro fails for any reason, the user cannot perform the function or cannot make updates.

ASM source member LCPXSMA2 in the LCPCNTL data set provides the interface to RACF services and issues the RACHECK macro by using the RACF class APPL and an 8-byte resource name. The resource name is constructed as follows:

- **LCP** – a fixed resource name prefix selected by BMC for LOCAL COPY PLUS RACF validation.
- **function** – the first character of the LOCAL COPY PLUS function to be validated.
- **imsid** – the one- to four-character IMSID of the user to be validated.

⚠️ **Note**

When the function character is L (for example, for general access to the LOCAL COPY PLUS ISPF panels), the IMSID will always be set to CP2@.
To define the individual resource names to the RACF class APPL, use the RACF (or equivalent) RDEFINE command.

For example, to control general access to the LOCAL COPY PLUS ISPF panels, use LCPLCP2@. To control update access to LOCAL COPY PLUS route-lists for IMSID IMSP, use LCPRIMSP.

**Control update access to LOCAL COPY PLUS route-lists for IMSID IMSP**

```
RDEFINE APPL LCPRIMSP UACC(READ)
```

To grant RACF UPDATE authority to authorized user IDs, use the RACF (or equivalent) PERMIT command.

For example, to permit update access to LOCAL COPY PLUS route-lists for the IMSID IMSP, enter the following PERMIT command:

```
PERMIT LCPRIMSP CLASS(APPL) ID(userid) ACCESS(UPDATE)
```

### Setting LOCAL COPY PLUS options

This section describes procedures for setting the LOCAL COPY PLUS IMSID options, Destination Entries, and Copy Table Entry options.

Use the following general guidelines when you set the LOCAL COPY PLUS options:

- You can replace LCPTTRAN1 with the name of your choice. If you change the name, ensure that you also change it in the LOCAL COPY PLUS options and that you update all references in LCPCNTL members LCPMFS22 and LCPMFS32.
- If you specify a SEGSIZE value, it must be at least 2048 bytes.
- If you specify a SEGNO value, it must be 50 or more. If you use Routing Lists, SEGNO should be set to zero.
- For the transaction to function properly, you should define it as *response mode*. You should define terminals that use the system administrator panels as `TRANRESP` in the IMSGEN.
- LCPTTRAN1 should not be pre-loaded.
- If you are operating in a shared queues environment (CQS) and you want to ensure that LCPTTRAN1 runs on the originating system, specify `SERIAL=YES`.

### Setting LOCAL COPY PLUS IMSID options

This section provides guidelines for setting the LOCAL COPY PLUS IMSID options.

Review the LOCAL COPY PLUS options and choose appropriate settings for your site.
• Use the I command on the LOCAL COPY PLUS Primary Menu to select the default IMSID or insert a new IMSID.

• If your IMS/VS Resident Library contains more than one IMS/VS nucleus and you want LOCAL COPY PLUS to be active on only one system, you can create an IMSID options module for each IMS/VS nucleus in the Resident Library and deactivate LOCAL COPY PLUS for those which will not be initially using the product. Specify N for the global option Auto-start LCP/V3 at IMS initialization to deactivate LOCAL COPY PLUS.

• Review the IMSID options and update key parameters and values such as the PF Key number, the transactions name(s), the IMS/VS Resident Library data set name, and the LOCAL COPY PLUS PDX data set name.

• Use PDX Data Set Option on the Utilities panel to allocate and initialize the LOCAL COPY PLUS PDX library.

Specifying LOCAL COPY PLUS Destination Entries

Depending on whether you choose to centrally administer the Destination Entries or delegate maintenance to end users, you should set the appropriate values to define the desired printer, display, or destination attributes.

You do not need to set Destination Entries for those devices that match the destination defaults that are defined in the LOCAL COPY PLUS options.

You can use option 1 of the Maintenance Menu to define and update Destination Entries in the PDX library, or you can use the various LOCAL COPY PLUS panels under IMS to create and update Destination Entries. For more information, see the LOCAL COPY PLUS Reference Manual.

Setting LOCAL COPY PLUS Copy Table Entry options

Depending on whether you choose to centrally administer the Copy Table Entries or delegate maintenance to end users, you should set the appropriate values to define the desired user copy options.

You should also define at least one Copy Table and update the options to specify the same Copy Table suffix.

You can use option 2 of the Maintenance Menu to select a Copy Table and update the Copy Table Entry options in the LOCAL COPY PLUS PDX data set, or you can use the various LOCAL COPY PLUS panels under IMS to create and update Copy Table Entries. For more information, see the LOCAL COPY PLUS Reference Manual.
Customizing Message Advisor for IMS

This section describes customization tasks that are unique to Message Advisor for IMS. Customization refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered in this section:

- Overview of customizing Message advisor for IMS (see page 179)
- Message Advisor customization worksheet (see page 179)
- Adding Message Advisor to TSO/ISPF (see page 181)
- Limiting access to Message Advisor (see page 184)
- Allocating Message Advisor data sets (see page 190)
- Setting the Message Advisor options (see page 193)
- Setting the Message Advisor QPF options (see page 200)
- Adding VTAM parameters (see page 201)
- Installing the QPF Test Applications (see page 210)
- Installing the Message Advisor Server (see page 212)
- Bringing up your IMS system (see page 212)
- Verifying Message Advisor installation (see page 213)

Overview of customizing Message advisor for IMS

You should complete the customization tasks after you have installed and configured the product libraries through the Installation System.

For information about installing and configuring the product libraries, see the Installation System documentation.

⚠️ Note

No configuration tasks were performed for Message Advisor.

The customization tasks that are presented are unique to Message Advisor.

Message Advisor customization worksheet

Refer to the following worksheet as you work through the customization process for Message Advisor:
### A Sample Table of Contents

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
</table>
| 1    | Provide access to the ISPF interface through a CLIST or through an ISPF options menu. | • Accessing Message Advisor from an ISPF options menu (see page 181)  
• Accessing Message Advisor from a CLIST (see page 181)  
• Accessing Message Advisor from an ISPF options menu (see page 181)  
• Allocating a request library for Message Advisor (see page 183) |
| 2    | Limit access to Message Advisor through an internally coded list, a SAF product, or an ACF2 product. | • Limiting access to Message Advisor (see page 184)  
• Implementing an internally coded list (function,userid, imsid,subfunction authorization) (see page 185)  
• Implementing a SAF product (see page 188)  
• Implementing an ACF2 product (see page 189) |
| 3    | Allocate Message Advisor data sets. | Allocating a request library for Message Advisor (see page 183) |
| 4    | Use the CUSTOMIZE command to set the Message Advisor options. | Setting the Message Advisor options (see page 193) |
| 5    | Use the QPF_OPTIONS command to set the Message Advisor QPF options. | Setting the Message Advisor QPF options (see page 200) |
| 6    | Add VTAM parameters. | • Adding VTAM parameters (see page 201)  
• Adding VTAM parameters for a single-CPU environment (see page 202)  
• Adding VTAM parameters for a multiple-CPU environment (see page 204) |
| 7    | (optional, but recommended) Install the QPF Test Applications. | Installing the QPF Test Applications (see page 210) |
| 8    | Install the Message Advisor Server. | Installing the Message Advisor Server (see page 212) |
| 9    | To confirm proper installation, bring up IMS. | Bringing up your IMS system (see page 212) |
| 10   | Test your installation. | • Verifying Message Advisor installation (see page 213)  
• Performing the batch IVP for Message Advisor (see page 214)  
• Performing the online IVP for Message Advisor (see page 219)  
• Performing the IVP for QPF (see page 223) |
Adding Message Advisor to TSO/ISPF

This section describes the procedures for adding Message Advisor to TSO/ISPF.

You can install the online interface so that you can invoke it from a CLIST or from an ISPF options menu. For more information, see Accessing Message Advisor from a CLIST (see page 181) and Accessing Message Advisor from an ISPF options menu (see page 181).

Accessing Message Advisor from a CLIST

A sample CLIST that provides access to the online interface using LIBDEF is available in the SAMP library. You can copy member QMRCLIST of the SAMP library into your CLIST library and update the following data set names to reference your data sets:

- &MAQLLIB
- &MAQMLIB
- &MAQPLIB
- &MAQTLIB

Accessing Message Advisor from an ISPF options menu

Accessing Message Advisor from an ISPF options menu requires that you pre-allocate the necessary ISPF data sets to the user.

You must add the following libraries to the TSO logon procedure for each user who requires access to Message Advisor:

- Load library (ISPLLIB)
- Panel library (ISPLLIB)
- ISPF message library (ISPMLIB)
- ISPF table library (ISPTLIB)
- Sample library (MAQSAMP)

⚠️ Note

There is an additional task related to accessing Message Advisor from an ISPF options menu. For more information, see Allocating a request library for Message Advisor (see page 183).

Message Advisor contains a hidden panel that allows you to specify many ISPF default product values. The panel is located in member QMRPUSER of the MAQSAMP library. Review the member to customize the ISPF interface default values for the product. Comments are included in the member to assist you.
The following figure shows a sample ISPF/PDF Primary Option Menu that has been modified to access Message Advisor.

**Sample modifications to ISPF/PDF Primary Option Menu**

```plaintext
%-----------------------  ISPF/PDF PRIMARY OPTION MENU  -----------------
%OPTION  ===>                                                           +
%  0 +ISPF PARMS      - Specify terminal and user parameters
%  1 +BROWSE          - Display source data or output listings
%  2 +EDIT            - Create or change source data
%  3 +UTILITIES       - Perform utility functions
%  4 +FOREGROUND      - Invoke language processors in foreground
%  5 +BATCH           - Submit job for language processing
%  6 +COMMAND         - Enter TSO command or CLIST
%  7 +DIALOG TEST     - Perform dialog testing
%  C +CHANGES         - Display summary of changes for this release
% MAQ +Message Advisor - BMC Message Advisor
%  Q +SDSF            - Spool Display and Search Facility
%  S +SMP/E           - New Version of SMP
%  T +TUTORIAL        - Display information about ISPF/PDF
%  X +EXIT            - Terminate ISPF using log and list defaults
%+Enter%END+command to terminate ISPF.
%
}INIT

HELP = ISR00003
&ZPRIM = YES /* ALWAYS A PRIMARY OPTION MENU */
&ZHTOP = ISR00003 /* TUTORIAL TABLE OF CONTENTS */
&ZHINDEX = ISR91000 /* TUTORIAL INDEX - 1ST PAGE */
}PROC
&ZSEL = TRANS( TRUNC (&ZCMD, '.')
  0,'PANEL(ISPOPTA)'  
  1,'PGM(ISRBRO)' 
  2,'PGM(ISEDIT)'
  3,'PANEL(ISRUTIL)'
  4,'PANEL(ISRFPA)'
  5,'PGM(ISRJB1) PARM(ISRJPA) NOCHECK'
  6,'PANEL(ISRTSOT)' 
  7,'PGM(ISRYXDR) NOCHECK'
 C,'PGM(ISPTUTOK) PARM(ISR00005)'
 MAQ,'PANEL(QMRP0000) NEWAPPL(QMR1)'
 Q,'PANEL(ZSDSSFOPT) NEWAPPL(ISF)'
 S,'PGM(GIMISCV) PARM(&ZCMD) NEWAPPL(SMP2)'
 T,'PGM(ISPTUTOR) PARM(ISR00000)'
  ' ' ' ' ' ' ' ' ' ' ' ' ' '
 X,'EXIT'
  ' ' ' ' ' ' ' ' ' ' '+,'?' }
&ZTRAIL = .TRAIL
IF (&OPT = 'Q')

&ZSEL = 'PGM(ISFISP) NOCHECK NEWAPPL(ISF)'
```

BMC System Administration for IMS, version 2.7.00
Allocating a request library for Message Advisor

To allocate a request library for Message Advisor, perform the following steps:

1. Select the Message Advisor ISPF menu.
   From the ISPF/PDF Primary Option Menu, select the Message Advisor option or type TSO 
   QMRCLIST on the Command line and press Enter.
   The Message Advisor banner panel is displayed. Press Enter to display the Message 
   Advisor Primary Menu.

   **Message Advisor Primary Menu**
   
   File  Session  Display  Help
   -----------------------------------------------------------------------------
   Message Advisor - Primary Menu  Product Level: Vn.n.nn
   
   Select one of the following. Then press Enter.
   
   1. Build and execute Message Advisor requests
      Request library bmcnode.REQUEST
   2. Display and/or dequeue specific IMS messages
   3. Display statistics for the IMS messages queues
   4. List IMS log/checkpoint history
   5. Customize Server and IMS options
   6. Execute Message Advisor and IMS commands
   7. BMC Software Product Authorization by CPU ID
   8. Queue Protection Facility
   9. Analyzer Display for Shared Queues

   IMSID . . . . Q22P+ (for options 2, 3, 4, 6, 8, 9)
   Server name . . QMRP+ (all options)
   '+' following an entry field indicates that the PROMPT action is available.
   (c) Copyright 2001 BMC Software, Inc. as an unpublished licensed work.
   All rights reserved.

2. Type 1 in the choice entry field to build and execute a Message Advisor request.
3. In the Request library field, type the name of the new partitioned data set in which you want 
   the Message Advisor request to reside and press Enter.
   The Request Library Create panel is displayed.
   **Request Library Create panel**
   
   Request Library Create
   | Data set information
3. | Data set name . . . bmcnode.REQUEST |
   | Volume serial . . . ______ (optional, for new data set only) |
   | Generic unit  . . . ________ (optional, for new data set only) |

   Space information (for new data set only)
   | Units . . . . . . TRKS (BLKS, TRKS, or CYLS) |
   | Primary quantity  . . 10__ |
   | Secondary quantity. . 5___ |
   | Directory blocks .. 20__ |

   DCB information (for new data set only)
   | Record format . . . FB_ (F,FB,FA,FM,FBA,FBM,V,VB,VA,VM,VBA,VBM) |
   | Logical record length 80___ (80-255 recommended) |
   | Block size . . . . 6160__ |

   Command ===> _______________________________________________________

4. Accept or change the information on the Request Library Create panel and press Enter.
   The Sample List pop-up panel is displayed.

   **Sample List pop-up panel**

   File  Session  Display  Help
   ==============================================================
   Member List - bmcnode.REQUEST
   ==============================================================
   Sample List

   | Select (type a '/') one of the following samples. |
   | Then press Enter. Line 001 of 017 |

   . (None - create a new request) |
   . Automatic Requeue after COLD Start |
   . Displaying statistics and master messages |
   . Dequeuing all messages: One destination |
   . Dequeuing selected messages: Multiple destinations |
   . Dequeuing a specific message |
   . Displaying message queue statistics |
   . Displaying destination queue information |
   . Displaying destination information |
   Command ===> _____________________________________________

   Type a slash ('/') next to None and press END.
   The Insert Command Set pop-up panel is displayed.

5. Press END twice to return to the Message Advisor Primary Menu.

**Limiting access to Message Advisor**

This section describes the procedures for limiting access to Message Advisor.
By default, access to Message Advisor is unlimited. To restrict product usage, you must take steps to protect the functions that you want to restrict.

Under most circumstances, you do not have to set security when initially installing Message Advisor. Therefore, you may want to defer setting security until you have reviewed the various security methods.

Message Advisor allows you to secure product features through the following methods:

- Internally coded list
  For more information, see Implementing an internally coded list (function,userid,imsid, subfunction authorization) (see page 185).
- External security program such as System Authorization Facility (SAF) or ACF2 supported by RACF and similar security products
  For more information, see Implementing a SAF product (see page 188) or Implementing an ACF2 product (see page 189).

**Implementing an internally coded list (function,userid,imsid, subfunction authorization)**

You can use an internally coded list of function,userid,imsid,subfunction authorization entries to control access to Message Advisor functions.

The default is to allow any user to access any function with any IMSID through a masked authorization entry.

The following table identifies the Message Advisor functions that you can secure:

**Message Advisor functions that can be secured through an internally coded list**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Subfunction</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSRV</td>
<td>Create and modify Server options during options customization</td>
<td>None</td>
</tr>
<tr>
<td>CIMS</td>
<td>Create and modify IMS options during options customization</td>
<td>None</td>
</tr>
</tbody>
</table>
| REQUEUE  | Requeue messages to the IMS message queues (subfunctions are two-character codes) | First character:  
  - C—COLD  
  - E—EREFAIL  
  - R—REPROCESS  
  - F—FILE  
  Second character:  
  - V—VALIDATE  
  - E—EXTRACT  
  - R—REQUEUE |
| DEQUEUE  | Dequeue messages from the IMS message queues | None |
### Function Description Subfunction

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Subfunction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISPLAY</td>
<td>Display information about the IMS message queues</td>
<td>S—Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Q—Destination Queues</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D—Destination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R—Record</td>
</tr>
<tr>
<td>IMSCMD</td>
<td>Submit Message Advisor and IMS commands</td>
<td>Subfunctions are three-character IMS command abbreviations</td>
</tr>
<tr>
<td>QPF_ACTION</td>
<td>Access the QPF_ACTION function</td>
<td>None</td>
</tr>
<tr>
<td>QPF_LIST</td>
<td>Access the QPF_LIST function</td>
<td>None</td>
</tr>
<tr>
<td>QPF_OPTIONS</td>
<td>Access the QPF_OPTIONS function</td>
<td>None</td>
</tr>
<tr>
<td>UNLOAD</td>
<td>Unload messages from the IMS message queues</td>
<td>None</td>
</tr>
<tr>
<td>CANCEL</td>
<td>Cancel an active command</td>
<td>None</td>
</tr>
<tr>
<td>LIST</td>
<td>List SLDS, OLDS, and checkpoints</td>
<td>None</td>
</tr>
</tbody>
</table>

### To limit access to Message Advisor functions through an internally coded list

1. Code the function,userid,imsid,subfunction entries of the ASM source member (MAQXSM0) of the MAQSAMP library to enable or deny access. The ASM source member provides the interface to the internally coded list.

   **Note**

   You can use an asterisk (*) as a wildcard character to include masking entries in the authorization list.

   Use the $AUID macro instruction to specify an authorization entry as follows:

   ```
   label $AUID function,userid,imsid,access-flag,subfunction
   ```

   The following table describes the terms that are specified in the authorization entry.

   **$AUID macro instruction terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>An optional symbolic name</td>
</tr>
<tr>
<td>function</td>
<td>One of the protected functions that are listed here (see page 185)</td>
</tr>
<tr>
<td></td>
<td>Use an asterisk (*) to indicate all functions.</td>
</tr>
<tr>
<td></td>
<td>You can abbreviate a function to the underscored character that is shown here (see page 185). For example, you can abbreviate REQUEUE to R.</td>
</tr>
</tbody>
</table>
1. Term Description

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userid</td>
<td>A specific userID or userID mask. The valid range is from one to eight characters. Use an asterisk (*) to indicate all userIDs.</td>
</tr>
<tr>
<td>imsid</td>
<td>A specific IMSID that has been defined through IMS options specification or an IMSID mask. The valid range is from one to four characters. Use an asterisk (*) to indicate all IMSIDs.</td>
</tr>
<tr>
<td>access-flag</td>
<td>Y or N depending on whether the user can access the function with the specified IMSID</td>
</tr>
<tr>
<td>subfunction</td>
<td>Keyword or parameter of the command that is to be restricted</td>
</tr>
</tbody>
</table>

Note

Only the DISPLAY, IMSCMD, and REQUEUE commands support subfunction security.

Include as many $AUID entries as necessary in the appropriate portion of the source member (after label MAQXTABL in source member MAQXSMA0). Review the default example entries and remove those that are inappropriate for your security requirements. The exit for the internally coded list may present a message by setting R0 and R1 before returning. A message may be returned regardless of whether access is granted or denied. In the QMRXSMA0 sample exit, if R0=0 no message is presented when access is allowed and a generic message is presented when access is denied. Use R0 and R1 as follows:

- R0 points to the message buffer
- R1 contains the message length

The authorization process searches the table from top to bottom and left to right. The first match determines the authorization. Generalized authorizations at the top or left of the list will nullify specific authorizations at the bottom or right of the list. You should place specific entries before general entries. For example, you might want to limit USERABC’s access so that he can perform all functions, but only with the IMSID IMST. At the same time, you may want to let all other users access all other functions.

2. Code the $AUID macros as shown in the following figure.

$AUID macro coding

$AUID *,USERABC,IMST,Y
$AUID *,USERABC,*,N
$AUID *,*,*,Y

The entries perform the following functions:

- The first entry enables USERABC to access all product functions with the IMSID IMST.
- The second entry prohibits USERABC from accessing any product functions with any other IMSID.
- The third entry enables all other users to access all other functions with all other IMSIDs.
Subfunction security adds an additional parameter to $AUID for the DISPLAY, IMSCMD, and REQUEUE commands. The following figures show examples of subfunction security.

Security for the DISPLAY command

|$AUID DISPLAY,\*,\*,\*,Y,S$ <- allow TYPE=STATISTICS display
|$AUID DISPLAY,\*,\*,\*,N,R$ <- prevent TYPE=RECORD display
|$AUID DISPLAY,\*,\*,\*,Y$ <- allow all other displays

Security for the IMSCMD command

|$AUID IMSCMD,\*,\*,\*,Y,D*$ <- allow everyone to use /DIS
|$AUID IMSCMD,IMSORP,\*,\*,C\*E$ <- allow user 'IMSORP' to use /CHE
|$AUID IMSCMD,\*,\*,N,C\*E$ <- deny others the use of /CHE
|$AUID IMSCMD,\*,\*,\*,Y$ <- allow everyone to use all other commands

Security for the REQUEUE command

|$AUID REQUEUE,\*,\*,\*,N,C$ <- prevent TYPE=COLD requeues
|$AUID REQUEUE,\*,\*,\*,Y,*E$ <- allow MODE=EXTRACT requeues
|$AUID REQUEUE,\*,\*,\*,N$ <- prevent all other requeues

3. Use JCL similar to that provided in MAQ CNTL member MAQ#SMA0 to assemble the authorization entries and implement the internally-coded security authorization list. If you are using SMP/E maintenance for Message Advisor, you need to use CNTL member MAQ#SMPE to apply the QMRXSMA0 security exit as a usermod. The control statements are in SAMP member MAQU007.

If you attempt to perform a function that is specified in an authorization entry, the product scans the internally coded list. If the product does not find a match or if the matched entry denies access, you cannot perform the function or make changes.

Implementing a SAF product

Message Advisor supports SAF security, which is supported by RACF and similar security products.

Member QMRXSMA1 of the MAQSAMP library provides a sample SAF security exit. To use this exit, edit member QMR#SMA0 of the CNTL library, change the EXEC ASMXCL statement to ASM=QMRXSMA1, and submit the statement.

If you are using SMP/E maintenance for Message Advisor, then you need to use CNTL member MAQ#SMPE to maintain the QMRXSMA1 security exit. The control statements are in SAMP member MAQU007.
You can add a new SAF security class for Message Advisor by updating the SAF class descriptor table (CDT) and the MVS router table. See the appropriate product manuals for instructions on defining and activating new classes.

The following figure shows a sample SAF CDT definition:

```
QMANAGER ICHERCDE CLASS=Q#MGR,ID=xxx,POSIT=x
MAXLNTH=44,FIRST=ANY,OTHER=ANY,
OPER=NO,DFTUACC=NONE,DFTRETC=8
```

The following figure shows a sample router table definition:

```
ICHRFRTB CLASS=Q#MGR,ACTION=RACF
```

The following figure shows sample resource definitions using default resource names:

```
RDEFINE Q#MGR IMSA.REQUEUE.* UACC(NONE)
RDEFINE Q#MGR IMSA.DISPLAY.* UACC(READ)
RDEFINE Q#MGR IMSA.IMSCMD.CHE UACC(NONE)
```

The following figure shows a sample permission:

```
PERMIT IMSA.REQUEUE.* CLASS(Q#MGR) ID(userid)
ACCESS(READ)
```

**Implementing an ACF2 product**

Message Advisor supports ACF2 security, which is supported by RACF and similar security products.

To implement ACF2 security, map resource class Q#MGR to a three-character ACF2 generalized resource type, as shown in the following example:

```
SET Control(GSO)
INSERT CLASMAP.Q#MGR ENTITYLEN(100) RESOURCE(Q#MGR) RSRCTYPE(MAQ)
```

In the example, .Q#MGR can be any suffix that follows site conventions for naming Global System Options (GSO) records, and MAQ can be any three-character resource type that follows site conventions.

After you map resource class Q#MGR, issue the following MVS command:
F ACF2,REFRESH(CLASMAP)

Alternatively, you can add a new ACF2 security class for Message Advisor by specifying a valid ACF2 resource type for the CLASS keyword in the ACF2 class descriptor table (CDT) and the MVS router table. See the appropriate product manuals for instructions on defining and activating new classes.

The following figure shows a sample ACF2 CDT definition:

```
QMANAGER ICHERCDE CLASS=Q#MGR,ID=xxx,POSIT=x
MAXLTH=44,FIRST=ANY,OTHER=ANY,
OPER=NO,DFTUACC=NONE,DFTRETC=8
```

The following figure shows a sample router table definition:

```
ICHRFRTB CLASS=Q#MGR,ACTION=RACF
```

Allocating Message Advisor data sets

This section describes the steps for allocating the data sets that are required for Message Advisor processing.

JCL for allocating the data sets is available in member QMR#ALLO of the MAQCNTL library.

The following table lists the Message Advisor data sets that you can allocate.

<table>
<thead>
<tr>
<th>Data set</th>
<th>Sample data set name</th>
<th>Must match customization options parameter</th>
<th>Data set organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECKPOINT</td>
<td>hlq.iii.ckpt</td>
<td>CHECKPOINT_DSN</td>
<td>VSAM RRDS</td>
</tr>
<tr>
<td>EXTRACT</td>
<td>hlq.iii.extract</td>
<td>EXTRACT_DSN</td>
<td>SEQ</td>
</tr>
<tr>
<td>UNLOAD</td>
<td>hlq.iii.unload</td>
<td>UNLOAD_DSN</td>
<td>SEQ</td>
</tr>
<tr>
<td>SCRAP</td>
<td>hlq.iii.scrap</td>
<td>SCRAP_DSN</td>
<td>SEQ</td>
</tr>
</tbody>
</table>

⚠️ **Note**

You must preallocate the Checkpoint data set. You can specify the other data sets at execution time.

The *hlq* variable in the following table represents your site’s high-level qualifier, and the variable *iii* represents your site-specific IMSID.
The data sets that you allocate must meet the following requirements:

- A unique CHECKPOINT data set is required for each IMSID that you specify. Message Advisor Checkpoint Tracking uses the CHECKPOINT data set to maintain a record of checkpoints for use during requeue processing. When you install the Message Advisor libraries in the IMS control region, Message Advisor Checkpoint Tracking is automatically activated.

Note

For the SPILL data sets that are described below, you can specify the data sets when you execute the REQUEUE command. To create the SPILL data sets at command execution time, use the SPILL prefix.

- A SPILL1 data set may be required for each IMSID that you specify. Message Advisor uses the SPILL1 data set during a REQUEUE TYPE=COLD/EREFAIL/REPROCESS to hold overflow from main storage for checkpoint records. If overflow occurs and this data set is not available, the requeue process fails. The SPILL1 data set is required if a requeue exhausts the extended private storage.

- A SPILL2 data set is required for each IMSID that you specify. Message Advisor uses this data set during a REQUEUE TYPE=EREFAIL/REPROCESS to hold log data for sorting. The SPILL2 data set is required if a requeue exhausts the extended private storage.

- A unique SPILL3 data set is required for each IMSID that you specify. Message Advisor uses the SPILL3 data set during a REQUEUE TYPE=EREFAIL/REPROCESS that begins from a SNAPQ to hold overflow from main storage. The SPILL3 data set contains 01, 03, and 3X log records. The SPILL3 data set is required if a requeue exhausts the extended private storage.

- A unique SPILL4 data set is required for each IMSID that you specify. Message Advisor uses the SPILL4 data set during a REQUEUE TYPE=EREFAIL/REPROCESS to hold overflow from main storage. The SPILL4 data set contains 01 and 03 log records. The SPILL4 data set is required if a requeue exhausts the extended private storage.

Note

For the next three data sets, you can specify...
• The UNLOAD command set requires a data set to which messages will be unloaded. You can specify the UNLOAD data set when you set the Message Advisor options, or you can specify it when you execute the UNLOAD command. If you specify the data set at command execution time, use the OUTPUT subcommand. For information about the data set characteristics, see member QMR#ALLO of the MAQCNTL library. For more information about the UNLOAD command, see the Message Advisor for IMS User Guide.

• An EXTRACT data set is optional for each IMSID that you specify. You can supply the EXTRACT data set when you set the Message Advisor options, or you can specify it when you execute the EXTRACT subcommand on a REQUEUE command. For information about the data set characteristics, see member QMR#ALLO of the MAQCNTL library. The EXTRACT data set is required if you specify REQUEUE MODE=EXTRACT, which copies messages into the EXTRACT data set. You can use these messages later as input to a requeue if you specify REQUEUE TYPE=FILE. For more information about the REQUEUE command, see the Message Advisor for IMS User Guide.

• A SCRAP data set is optional for each IMSID that you specify. You can supply the SCRAP data set when you set the Message Advisor options, or you can specify it when you execute the SCRAP subcommand on a REQUEUE command. For information about the data set characteristics, see member QMR#ALLO of the MAQCNTL library. If the SCRAP data set is available during a requeue, Message Advisor writes messages that cannot be requeued because of an exception condition to the data set. An example of an exception condition is an LTERM or transaction that no longer exists in IMS. For more information about the REQUEUE command, see the Message Advisor for IMS User Guide.

To allocate the data sets that are required for Message Advisor processing

1. Modify the data set names and volume serial numbers to comply with your site’s requirements.

⚠️ Note

Do not change data set organization, logical record length, or block size.
2. Allocate the data sets that are listed in the table Message Advisor data sets that can be allocated (see page 190).
   The data set names that you assign must match the names that you specify when you set the Message Advisor options module keywords.
   For more information about the Message Advisor options module, see Setting the Message Advisor options (see page 193).

3. Set the space parameter.
   Because the amount of data to be processed is generally unknown, the value that you specify will be an estimate. You need enough space to hold each 4002, 01, 03, and 3X IMS log record from the last DUMPQ or SNAPQ to the end of file input. BMC suggests setting the space at 10 cylinders primary and 50 cylinders secondary.

   **Note**
   The Message Advisor Checkpoint Tracking data set requires only one track.

4. Change $iii$ to your site-specific IMSID.

   **Note**
   When you allocate the data sets, record the IMSID and the data set name. The IMSID that you specify in the Message Advisor options must match the IMSID that you specify when you allocate the data sets. You will also need to know the data set names when you set the Message Advisor options.
   For more information about the Message Advisor options, see Setting the Message Advisor options (see page 193).

---

**Setting the Message Advisor options**

This section describes how to use the CUSTOMIZE command and its subcommands to set Message Advisor options.

**Note**
For complete command syntax information, see the *Message Advisor for IMS Reference Manual*. 
The Message Advisor Queue Manager utilities (QMR) component requires an options module with options that are specific to each Message Advisor Server. Additionally, each IMS system that Message Advisor serves requires options that are unique to the IMS system. The CUSTOMIZE command and its SERVER_OPTIONS and IMS_OPTIONS subcommands provide this information to Message Advisor. The CUSTOMIZE command also includes a LIST_OPTIONS subcommand that displays options parameters.

You can use the CUSTOMIZE command to add, update, or delete the Message Advisor SERVER_OPTIONS and IMS_OPTIONS as often as necessary. Member QMR#OPTS of the MAQCNTL library contains sample JCL for specifying the options - see figure Setting Message Advisor options. (see page 196)

⚠️ **Note**

If you already have Q:MANAGER-defined jobs to set the options, you can use that JCL.

The SERVER_OPTIONS subcommand defines a particular Message Advisor Server and its unique parameters (for example, the VTAM ACB name).

The IMS_OPTIONS subcommand keywords let you perform the following tasks:

- Specify IMS systems that a Message Advisor Server will serve
- Specify parameters that are unique to each IMS system (for example, the IMS RECON data sets)
- Specify whether to activate the virtual LTERM creation feature
- Establish an automatic requeue, define parameters, and identify the required MVS command that initiates the automatic requeue

⚠️ **Warning**

BMC recommends that you use the automatic requeue feature only with REQ_PROMPT=YES. Although it is possible to activate the automatic requeue feature with REQ_PROMPT=NO, after a normal IMS cold start Message Advisor will initiate a requeue with no operator supervision. Depending on the cause of the cold start, the checkpoint that Message Advisor automatically selects may not be the checkpoint that you need to accurately requeue your IMS messages.

The IMS_OPTIONS subcommand that is shown at the bottom of Setting Message Advisor options (see page 196) uses the AUTO_REQ and AUTO_REQ_CMD keywords.

Follow these guidelines when specifying the CUSTOMIZE command and its subcommands:
You can define multiple Message Advisor Servers and multiple IMS systems in the same options module. If multiple Message Advisor Servers will share the options module, the SERVER_OPTIONS keyword SERVER_NAME must be unique for each Message Advisor Server.

If you include multiple SERVER_OPTIONS subcommand sets, you must ensure that the SERVER_APPLID keyword for each set matches the ACBNAME field in the APPL definition that is designated for each VTAM domain.

To identify an IMS system, use the IMS_OPTIONS keyword IMSID. You can use more than one set of IMS_OPTIONS to designate different IMS systems. Each set must include a unique IMSID.

Assign a unique data set name for each data set that will hold IMSID information. Each data set name should be related to only one IMS system. For example, if your site includes three IMS systems, you must assign different names to each Message Advisor Checkpoint Tracking data set, each spill data set, and so forth.

You must follow the command set syntax that is described below when building CUSTOMIZE command sets:

- If you type an asterisk (*) in column 1, the entire line of text becomes a comment. If you type a semicolon (;) anywhere in a line, any text on the line that follows the semicolon becomes a comment.
- The CUSTOMIZE command and its subcommands and keywords can begin in any column and are delimited with a comma. An equal sign (=) must follow keywords. Columns 72-80 should remain blank.
- To continue a string across multiple lines, the string must meet the following conditions:
  - The string must extend through the last valid column on the current line. For a standard 80-byte fixed length record, the last valid column is column 71.
  - The first non-blank character on the next line must be the delimiter that you typed at the beginning of the string.
- If a command consists of a string that extends across two lines and single quotation marks (‘) are used elsewhere in the string, the delimiter at the beginning of the character string must be a double quotation mark (’).
- You can specify a value that includes symbolic keywords with the following CUSTOMIZE command keywords:
  - AUTO_CMD_COLDCOM keyword
  - AUTO_CMD_COLDSYS keyword
  - AUTO_REQ_CMD keyword
  - All data set name keywords including CHECKPOINT_DSN, EXTRACT_DSN, RECON1_DSN, RECON2_DSN, RECON3_DSN, SCRAP_DSN, SPILL1_DSN, SPILL2_DSN, SPILL3_DSN, SPILL4_DSN, and UNLOAD_DSN

For all of these keywords, you can specify a value that includes the symbolic keyword %IMSID. The current IMSID replaces %IMSID.
For the EXTRACT_DSN, SCRAP_DSN, and UNLOAD_DSN keywords, you can specify a value that includes the symbolic keyword %USER. The current RACF userID of the requestor replaces %USER. The requestor is the TSO userID for an online server and the batch job name for a batch server.

A non-alphanumeric character must follow a symbolic keyword. If the keyword is followed by a percent sign (%) which is not part of another symbolic keyword, the trailing % will be removed and the following characters will be concatenated to the symbolic value.

The following figure shows sample JCL for setting the Message Advisor options.

\[\text{Note}\]

For complete command syntax information, see the *Message Advisor for IMS Reference Manual.*

If you already have Q:MANAGER-defined jobs to set the options, you can use that JCL.

### Setting Message Advisor options

```plaintext
//QMR#OPTS JOB (ACCT),'MAQ OPTIONS CUST'
<<<< MODIFY
//
// $BMCCHG P173384,CNTL ADD NEW KEYWORDS FOR AUTO REQ
// $BMCCHG P176777,CNTL MSG QUEUE STATISTICS 0176777
// $BMCCHG P178001,CNTL VIRTUAL_CREATE IMS OPTION 0178001
// $BMCCHG P184323,CNTL REMOVE LOAD BAL OPTIONS 0184323
/
/*
/* THIS SAMPLE JOB CAN BE MODIFIED AND EXECUTED TO CUSTOMIZE THE
/* OPTIONS MODULE FOR YOUR SERVER AND IMS SYSTEM
/* 1. THE STEPLIB DD INDICATES THE NAME OF THE LOAD
/* LIBRARY. (THIS LIBRARY WILL NEED TO BE CONCATENATED AHEAD
/* OF THE IMS.RESLIB IN THE STEPLIB OF YOUR Control REGION,
/* THEREFORE, IT MUST BE APF-AUTHORIZED)
/* 2. THE QMROPTS DD INDICATES WHERE THE OPTIONS MODULE 'QMRUOPT0'
/* IS PLACED, RECOMMEND PUTTING IT WITH THE OTHER Message Advisor
/* LOAD MODS
/* 3. CHANGE ALL REFERENCES TO QMRP TO THE NAME YOU CHOSE FOR YOUR
/* SERVER. (YOUR VTAM DEFINITIONS WILL NEED THE SAME CHANGES)
/* 4. CHANGE ALL REFERENCES TO QMRU TO THE ACBNAME PREFIX YOU
/* USE ON THE VTAM APPL STATEMENTS FOR YOUR Message Advisor
/* ISO SESSIONS
/* 5. CHANGE ALL REFERENCES TO IMSA TO YOUR IMSID.
/* 6. ALL DATA SETS WERE ALLOCATED IN THE ALLOCATION STEP
/* OPTIONS EXEC PGM=QMRCTL00,PARM="@@@@@@0,BATCH",REGION=2048K
```
CUSTOMIZE
SERVER_OPTIONS
SERVER_NAME=QMRP,
DEFAULT_SERVER=QMRP,
TITLE=C'Message Advisor',
SSCTNAME=QMR,
TRACE=2000,
SORTCORE=4096K,
SWAP=NO,
UPPERCASE=NO,
REQ_PROMPT=YES,
GRS_QNAME=QMANAGER,
SERVER_APPLID=QMRP,
VTAM_LOGMODE=QMANAGER,
VTAM_LU_PREFIX=QMRU,
WTO_DESC=X'0600',
WTO_ROUTCDE=X'4060'
IMS_OPTIONS
IMSID=IMSA,
RATE=0,
LOGCODE=EF,
AUTO_REQ=N,
AUTO_REQ_CMD=, ;SEE SAMPLE QMR$CMD1 IN QMR.SAMP
RECON1_DSN=IMSVS.IMSA.RECON1,
RECON2_DSN=IMSVS.IMSA.RECON2,
RECON3_DSN=IMSVS.IMSA.RECON3,
CHECKPOINT_DSN=BMCNODE.IMSA.CKPT,
EXTRACT_DSN=BMCNODE.IMSA.EXTRACT, 
UNLOAD_DSN=BMCNODE.IMSA.UNLOAD,
SCRAP_DSN=BMCNODE.IMSA.SCRAP,
SPILL1_DSN=BMCNODE.IMSA.SPILL1,
SPILL2_DSN=BMCNODE.IMSA.SPILL2,
SPILL3_DSN=BMCNODE.IMSA.SPILL3,
SPILL4_DSN=BMCNODE.IMSA.SPILL4,
VIRTUAL_CREATE=YES
IMSID=IMSB,
RATE=0,
LOGCODE=EF,
AUTO_REQ=N,
AUTO_REQ_CMD=, ;SEE SAMPLE QMR$CMD1 IN QMR.SAMP
AUTO_REQ_COLDCOM=NO,
AUTO_CMD_COLDCOM=,
AUTO_REQ_COLDSYS=NO,
AUTO_CMD_COLDSYS=,
RECON1_DSN=IMSVS.IMSB.RECON1,
RECON2_DSN=IMSVS.IMSB.RECON2,
RECON3_DSN=IMSVS.IMSB.RECON3,
CHECKPOINT_DSN=BMCNODE.IMSB.CKPT,
EXTRACT_DSN=BMCNODE.IMSB.EXTRACT,
UNLOAD_DSN=BMCNODE.IMSB.UNLOAD,
SCRAP_DSN=BMCNODE.IMSB.SCRAP,                    <==OPTIONAL
SPILL1_DSN=BMCNODE.IMSB.SPILL1,                  <==OPTIONAL
SPILL2_DSN=BMCNODE.IMSB.SPILL2,                  <==OPTIONAL
SPILL3_DSN=BMCNODE.IMSB.SPILL3,                  <==OPTIONAL
SPILL4_DSN=BMCNODE.IMSB.SPILL4,                  <==OPTIONAL
VIRTUAL_CREATE=YES
LIST_OPTIONS SERVER_NAME=QMRP
END
/*

To set the Message Advisor options

1. Rename the default Message Advisor Server as appropriate for your site.
   The PARM='@@@@@@@@,BATCH' provides the name of the default Message Advisor
   Server and specifies that this options job will run in batch. After you create a Message
   Advisor Server name, substitute that name for the default (@@@@@@@@) to obtain your
   values. You can only use the value @@@@@@@@ as the Message Advisor Server name
   when you execute the CUSTOMIZE command. Other Message Advisor commands require
   that you specify a Message Advisor Server name other than @@@@@@@@.

2. Modify the STEPLIB DD statement to recognize the APF-authorized library that contains the
   Message Advisor modules.

   ! Note
   If the library is not authorized, you will receive a system 047 abend.

3. Modify the QMROPTS DD statement to recognize a load library that will contain the
   QMRUOPT0 options module.
   You can use the same library as the one that is specified in the STEPLIB DD, or you can
   use a different load library.

   ! Note
   If desired, you can also add the QMROPTS DD statement to the IMS control
   region JCL to access the QMRUOPT0 load module.
   The QMRUOPT0 module must reside in a load library that is allocated in the
   control region. Message Advisor attempts to locate an MAQOPTS DD statement
   first. If it does not find an MAQOPTS DD statement, it attempts to locate a
   QMROPTS DD statement. If it does not find either statement, the QMRUOPT0
   module must be in the STEPLIB concatenation.

4. Use the CUSTOMIZE command to initiate a customization procedure.
You can repeat the subcommands and keywords for each Message Advisor Server or IMS system to be used. The following figure shows the sequence of the CUSTOMIZE command, its subcommands, and keywords.

**Note**

- For complete command syntax information, see the *Message Advisor for IMS Reference Manual*.
- When you set the Message Advisor options, the IMSID and data set names that you specify must match the IMSID and data set names that you specified during data set allocation. For more information about allocating Message Advisor data sets, see Allocating Message Advisor data sets (see page 190).
- You do not have to define all of your Message Advisor Servers and IMS systems during installation. You can perform this step at any time to redefine old systems or to create new systems.

**Structure of CUSTOMIZE command and subcommands**

```plaintext
//SYSIN DD *
CUSTOMIZE        This command indicates that an option customization is to be performed.

SERVER_OPTIONS  Repeat this subcommand and its keywords for each Message Advisor Server environment to be run.

•
•
•
•

keywords

•
•
•
•

IMS_OPTIONS      Repeat this subcommand and its keywords for each IMS system.

•
•

keywords

•
•

LIST_OPTIONS     Use this command to display options. You cannot have multiple LIST_OPTIONS in one command set.

END              This required command indicates the end of the command set.

/*
```
This step creates only one options module named QMRUOPT0, which contains entries for both Message Advisor Server and IMS options. This module can maintain multiple Message Advisor Servers and IMS options; however, all IMS systems that will be referred to by a Message Advisor Server must reside in the same QMRUOPT0 options module. If you do not want to share an options module between Message Advisor Servers, you must create different options libraries. To do so, specify these options libraries in the QMROPTS DD statement of the Message Advisor Server with which they will be associated.

Setting the Message Advisor QPF options

This section describes the steps for setting the Message Advisor Queue Protection Facility (QPF) component options.

Although QPF will be installed at the end of this task, you must also activate it. You can activate QPF now, or anytime after completing installation. BMC recommends that you activate QPF now so that it will be active when installation is complete.

To activate QPF, execute a QPF_OPTIONS command set that specifies ACTIVE=YES. You can use either of the following methods to activate QPF:

- provide a QPF_OPTIONS command set in the IMSVS.PROCLIB
  With this method, QPF will immediately activate whenever you restart IMS.
- submit a QPF_OPTIONS command set to the Message Advisor Batch Server
  With this method, QPF will only remain active until you restart IMS. After each IMS restart, you must resubmit a QPF_OPTIONS command set to reactivate QPF.

Note

For complete command syntax information, see the Message Advisor for IMS Reference Manual.

To set the Message Advisor QPF options

1. Determine how you want to activate QPF.

<table>
<thead>
<tr>
<th>If you want to activate QPF</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>By providing a QPF_OPTIONS command set in the PROCLIB</td>
<td>Step 2 (see page 200)</td>
</tr>
<tr>
<td>By submitting a QPF_OPTIONS command set to the Message Advisor Batch Server</td>
<td>Step 3 (see page 201)</td>
</tr>
</tbody>
</table>

2. Install a QPF_OPTIONS command set in the PROCLIB.
   a. Copy QPF@OPT1 from the MAQSAMP library and save it as QPFcccc (where cccc is your IMSID) in the PROCLIB of the IMS for which you want to activate QPF.
QPF@OPT1 contains a QPF_OPTIONS command set that specifies ACTIVE=YES. This command set also specifies the following information:

- The Monitor Phase begins at 0 percent of queue usage (immediately).
- The Protect Phase begins when queue usage reaches 50 percent.
- The Overflow Phase begins when queue usage reaches 80 percent.

b. Change the settings for the QPF_OPTIONS command set if desired.

At the next restart, QPF will be active in your IMS; however, the values that are specified in this QPF_OPTIONS command set are minimal and arbitrary. After you become familiar with QPF processing, modify the QPF_OPTIONS command set to reflect values that optimally address queue usage in your environment.

For more information about setting the QPF options, see the *Message Advisor for IMS User Guide* and the *Message Advisor for IMS Reference Manual*.

3. Submit a QPF_OPTIONS command set to the Message Advisor Batch Server.

**Note**

If you use this activation method, postpone this task until after you bring up IMS.

a. Select member QPF@OPT1 from the MAQSAMP library.
b. Submit a batch job to execute the command set.
   - Select member QMR#BJCL (or use existing Message Advisor Batch Server JCL).
   - Change the PARM parameter to match the Message Advisor Server name that you created when you set the Message Advisor options.
   - Change the STEPLIB DD to recognize the APF-authorized library that contains the Message Advisor modules.
   - Change the QMROPTS DD to recognize the library that contains the Message Advisor customized options module.

QPF will be active until you restart IMS. If you use this activation method, you must resubmit a QPF_OPTIONS command set after each IMS restart to reactivate QPF. The values that are specified in this QPF_OPTIONS command set are minimal and arbitrary. After you become familiar with QPF processing, modify the QPF_OPTIONS command set to reflect values that optimally address queue usage in your environment.

For more information about setting the QPF options, see the *Message Advisor for IMS User Guide* and the *Message Advisor for IMS Reference Manual*.

### Adding VTAM parameters

This section describes the procedures for setting Message Advisor VTAM parameters for single- and multiple-CPU environments.
1. **Note**

   If your site uses multiple CPUs and requires inter-CPU communication between Message Advisor ISPF sessions and the Message Advisor Server, see Adding VTAM parameters for a multiple-CPU environment (see page 204).

You can execute Message Advisor through an ISPF interface, batch jobs, or input from a write-to-operator with reply (WTOR).

The Message Advisor Server requires a VTAM logical unit (LU) 6.2 session for communication between the Message Advisor Server and the Message Advisor ISPF user session. Member QMR$APPL of the MAQSAMP library contains the sample statements that are shown in these procedures. Sample statements for both single- and multiple-CPU environments are included.

## Adding VTAM parameters for a single-CPU environment

To add VTAM parameters for a single-CPU environment, perform the following steps:

1. Create Message Advisor Server VTAM APPL definition statements and Message Advisor ISPF user session VTAM APPL definition statements for a single-CPU environment.
   a. Create Message Advisor Server VTAM APPL definition statements.
      
      The following figure shows statements that define the Message Advisor Server to VTAM.

      ```
      DEF QMRP APPC=YES,SECACPT=CONV
      LMDENT=0,DMINWNL=0,DMINWNR=10,DSESLIM=10,
      DRESPL=ALLOW,DLOGMOD=QMANAGER,MODETAB=QMGRMODE,
      ACBNAME=QMRP
      ```

      **Note**

      If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

      Follow these guidelines when creating Message Advisor Server VTAM APPL definition statements:
      - Add statements similar to the statements that are shown in the above figure to the SYS1.VTAMLST data set or its equivalent.
1. a. Do not assign the same name to the member in the SYS1.VTAMLST data set as that assigned to the logical unit (LU), which is displayed in columns 1 through 8 in the APPL statement in the above figure.

b. You must assign the **ACBNAME** field the same name that you specified for the SERVER_APPLID keyword when you set the Message Advisor options. For more information, see **Setting the Message Advisor options** (see page 193).

2. Create Message Advisor ISPF user session VTAM APPL definition statements.

The following figure shows statements that define the Message Advisor ISPF user sessions to VTAM.

### Defining concurrent Message Advisor ISPF sessions to VTAM

```plaintext
VBUILD TYPE=APPL
QMRP0001 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0001
QMRP0002 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0002
QMRP0003 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0003
```

**Note**

If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

The statements that are shown in the above figure define three possible concurrent Message Advisor ISPF user sessions. Follow these guidelines when creating Message Advisor ISPF user session VTAM APPL definition statements:

- Define one or more user sessions.
- The LU name labels must be unique within your VTAM network, whereas the **ACBNAME** fields must be unique within an MVS system.
- The first four characters of the **ACBNAME** operands must match the value that you specified for VTAM_LU_PREFIX when you set the Message Advisor options. The second four characters of the **ACBNAME** must appear as consecutive numbers, beginning with 0001, 0002, and so forth.

2. Assemble and link-edit the mode table.

A mode table is required for Message Advisor operations. The required parameters for the mode table are shown the following figure. Member QMRS.MODE of the MAQSAMP library contains a sample mode table.

### Parameters for required Message Advisor mode table

```plaintext
QMGRMODE MODETAB
QMANAGER MODEENT LOGMODE=QMANAGER,FMPROF=X'13', X
   TS.timer=X'07',PRIPROT=X'BO',
```

BMC System Administration for IMS, version 2.7.00

Page 203 of 284
Note
If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

Follow these guidelines when assembling and link-editing the mode table:

- Assemble and link-edit the mode table into SYS1.VTAMLIB or an equivalent data set.
- Before you assemble and link-edit the code, change the LOGMODE name to the name that you specified when you set the Message Advisor VTAM_LOGMODE options. For more information, see Setting the Message Advisor options (see page 193).
- The VTAM APPC interface will force all of the keywords (except RUSIZES) in the mode table that is shown in the above figure to their correct default values.
- The RUSIZES keyword indicates the size of the buffers that are used to transmit information between the Message Advisor Server and the Message Advisor ISPF user sessions. Since Message Advisor can transmit relatively large amounts of information, it is important to use large buffer sizes.

The default for non-APPC VTAM applications allows unlimited buffer sizes, whereas the default buffer size for VTAM APPC applications is 256 bytes. Using the default will result in poor Message Advisor user session response time.

The suggested value of X’8989’ specifies 4K buffers for transmissions from the Message Advisor Server to the ISPF user and for transmissions from the ISPF user to the Message Advisor Server.

- To move 4K transmission through SNA, the PCCU macro MAXDATA parameter must be at least 4130 for all NCPs through which this data may pass.

If the MAXDATA parameter is not this large or if VTAM errors occur, you must change the RUSIZES value to reduce the buffer size.

Adding VTAM parameters for a multiple-CPU environment

To add VTAM parameters for a multiple-CPU environment, perform the following steps:

Note
The Message Advisor Server and IMS must run on the same CPU. However, Message Advisor ISPF sessions can run on any CPU.
1. Create Message Advisor Server VTAM APPL definition statements, Message Advisor ISPF user session VTAM APPL definition statements, and CDRSC VTAM definition statements for a multiple-CPU environment.

VTAM definitions may be required on each CPU for multiple-CPU, cross-domain VTAM environments. The requirements depend on where the Message Advisor Server and the Message Advisor ISPF user sessions run, as described in the following table.

**VTAM definitions for the Message Advisor work load division**

<table>
<thead>
<tr>
<th>If you have a dual CPU with the work load divided as follows</th>
<th>Message Advisor needs the following VTAM definitions</th>
</tr>
</thead>
</table>
| MVST An MVS system executing most of the TSO processing (indicating where the Message Advisor ISPF user sessions will be used most often). For more information, see Step 1.a (see page 205), Step 1.b (see page 206), and Step 1.c (see page 207). | • VTAM APPL statements for the MVST Message Advisor ISPF user sessions that will be accessing the Message Advisor Server on MVSP  
• A VTAM CDRSC statement that defines cross-domain access to the Message Advisor Server that is executing on the MVSP system |
| MVSP An MVS system executing the IMSP control region (indicating where the Message Advisor Server will need to run) with limited TSO processing. For more information, see Step 1.d (see page 207), Step 1.e (see page 208), and Step 1.f (see page 209). | • A VTAM APPL statement for the Message Advisor Server that will run on MVSP to service the IMSP control region  
• VTAM APPL statements for any Message Advisor ISPF user session that will be accessing the Message Advisor Server from MVSP |

a. Create Message Advisor Server VTAM APPL definition statements for the MVST system.

The following figure shows statements that define the Message Advisor Server for the MVST system.

**Defining the Message Advisor Server for the MVST system**

```plaintext
VBUILD TYPE=APPL
QMR
APPL APPC=YES,SECACPT=CONV, X
LMDENT=0,DMINWNL=0,DMINWNR=10,DSESBLIM=10, X
DRESPL=ALLOW,DLOGMOD=QMANAGER,MODETAB=QMGRMODE, X
ACBNAME=QMR
```

⚠️ **Note**

If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

Follow these guidelines when creating the Message Advisor Server statements for the MVST system:
b. Create Message Advisor ISPF user session VTAM APPL definition statements for the MVST system.

The following figure shows statements that define the Message Advisor ISPF APPL for the MVST system.

**Defining Message Advisor ISPF APPL for the MVST system**

![VTAM APPL definition statements]

- **Note**

If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

Follow these guidelines when creating Message Advisor ISPF user session VTAM APPL definition statements for the MVST system:

- Add statements similar to the statements that are shown in in the preceding figure to SYS1.VTAMLST (or its equivalent) on the MVST system.
- Do not use a SYS1.VTAMLST member name that is the same as any LU name on any APPL or CDRSC statements.
- The LU name labels must be unique throughout your VTAM network, whereas the **ACBNAME** fields must be unique only within any MVS system.
1. **b.** The first four characters of the ACBNAME operands must match the VTAM_LU_PREFIX that you specified when you set the Message Advisor options. The second four characters must appear as consecutive numbers beginning with 0001, 0002, and so forth.

For more information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).

c. Create CDRSC VTAM definition statements for the MVST system.
The following figure shows statements that define the Message Advisor CDRSC for the MVST system.

**Defining Message Advisor CDRSC for the MVST system**

```
VBUILD  TYPE=CDRSC
QMRP    CDRSC   CDRM=MVSP
```

Follow these guidelines when creating CDRSC VTAM definition statements for the MVST system:

- Add statements similar to the statements that are shown in the preceding figure, to SYS1.VTAMLST on the MVST system to provide VTAM with cross-domain access to the Message Advisor Server that is executing on the MVSP system.

- The LU name label must match the LU name of the VTAM APPL statement that defines the Message Advisor Server on the MVSP system because VTAM definition only identifies where the named VTAM application resides.

d. Create Message Advisor Server VTAM APPL definition statements for the MVSP system.
The following figure shows statements that define the Message Advisor Server for the MVSP system.

**Defining the Message Advisor Server for the MVSP system**

```
VBUILD TYPE=APPL
QMRP    APPL APPC=YES,SECACPT=CONV,                                     X
        LMDENT=0,DMINWNL=0,DMINWNR=10,DSESLIM=10,                  X
        DRESPL=ALLOW,DLOGMOD=QMANAGER,MODETAB=QMGRMODE,            X
        ACBNAME=QMRP
```

**Note**

If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

Follow these guidelines when creating the Message Advisor Server VTAM APPL statement for the MVSP system:
1. Add statements similar to those that are shown in the preceding figure to define the Message Advisor Server for the MVSP system.

2. The LU name label must be unique throughout your network (except for CDRSC definitions on other systems that see the MVSP system).

3. The LU name label must match the name that you specified for SERVER_NAME.

4. The **ACBNAME** field must match the SERVER_APPLID that you specified when you set the Message Advisor options. For more information, see Setting the Message Advisor options (see page 193).

e. Create Message Advisor ISPF user session VTAM APPL definition statements for the MVSP system.

The following figure shows statements that define the Message Advisor ISPF APPL for the MVSP system.

**Defining Message Advisor ISPF APPL for the MVSP system**

```
VBUILD TYPE=APPL
QMRP0001 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0001
QMRP0002 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0002
QMRP0003 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0003
QMRP0004 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0004
QMRP0005 APPL APPC=YES,MODETAB=QMGRMODE,DLOGMOD=QMANAGER, X
   EAS=1,ACBNAME=QMRU0005
```

**Note**

If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

Follow these guidelines when creating the Message Advisor ISPF APPL statements for the MVSP system:

- Add statements similar to the statements that are shown in the preceding figure to SYS1.VTAMLST on the MVSP system to define any MVSP Message Advisor ISPF session that will access the Message Advisor Server on MVSP.

- The LU name labels must be unique throughout your VTAM network, whereas the **ACBNAME** fields must be the same as the **ACBNAME** fields on each of the other systems.
• The four-character prefix of the ACBNAME operands must match the
  VTAM_LU_PREFIX that you specified when you set the Message Advisor
  options. The second four characters must appear as consecutive numbers
  beginning with 0001, 0002, and so forth.

  For more information about setting the Message Advisor options, see Setting the
  Message Advisor options (see page 193).

f. Create CDRSC VTAM definition statements for the MVSP system.

The following figure shows statements that define the Message Advisor CDRSC for
the MVSP system.

**Defining the Message Advisor CDRSC for the MVSP system**

<table>
<thead>
<tr>
<th>VBUILD</th>
<th>TYPE=CDRSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>QMRT</td>
<td>CDRSC</td>
</tr>
<tr>
<td></td>
<td>CDRM=MVST</td>
</tr>
</tbody>
</table>

**Note**

If you already have Q:MANAGER-defined mode tables, you do not have to
create these VTAM APPL definition statements.

Follow these guidelines when creating CDRSC VTAM definition statements for the
MVSP system.

• Add CDRSC statements similar to the statements that are shown in the
  preceding figure to the SYS1.VTAMLST data set on the MVSP system to
  provide VTAM cross-domain access from the MVSP Message Advisor ISPF
  sessions to the Message Advisor Server on MVST.

• The LU name label must match the LU name of the VTAM APPL statement
  that defines the Message Advisor Server on the MVST system. This VTAM
  definition merely identifies where the named VTAM application resides.

**Note**

For multiple-CPU environments that have more than a dual CPU, add the
appropriate sets of VTAM definitions based on the Message Advisor
environments on the particular MVS system.

2. Assemble and link-edit the mode table.

A mode table is required for Message Advisor operations. The required parameters for the
model table are shown in the following figure. Member QMR$MODE of the MAQSAMP
library contains a sample mode table.

**Parameters for required Message Advisor mode table**
Note

If you already have Q:MANAGER-defined mode tables, you do not have to create these VTAM APPL definition statements.

Follow these guidelines when assembling and link-editing the mode table:

- You must assemble and link-edit the mode table into SYS1.VTAMLIB or an equivalent data set.
- Before you assemble and link-edit the code, change the LOGMODE name to the name that you specified when you set the Message Advisor VTAM_LOGMODE options. For more information, see Setting the Message Advisor options (see page 193).

Installing the QPF Test Applications

This section describes the steps for installing the Message Advisor QPF Test Applications.

The QPF Test Applications are programs that simulate various queue overflow conditions in order to test both the Message Advisor QMR functions and the QPF functions.

Note

Installing the QPF Test Applications is an optional task; however, BMC recommends that you install these test applications as part of the configuration process.

To install the QPF Test Applications in your IMS test environment:

1. Define the sample applications to your IMS system.
   You can use either of the following methods to define the sample applications:
1. Add the Test Application Stage1 definition to your IMS Stage1 source and perform an IMS SYSGEN. Member QPF$STG1 of MAQSAMP contains sample Stage1 source. Two batch message processing programs (BMPs) and one message processing program (MPP) with ten transactions are supplied. You can add additional transactions and change the definition names to meet your needs. Any name changes must be propagated through the remaining steps, where appropriate.

2. After reviewing the Test Application Stage1 definitions, use Message Advisor to add them to your IMS system. Make changes as needed for security. Make any appropriate definitions for transaction security using ACF2 or RACF.

3. Perform an IMS PSBGEN and ACBGEN. Member QPF#PSB of the MAQCNTL library contains a sample PSBGEN/ACBGEN job stream. This job uses MAQSAMP members QPF$PSB1, QPF$PSB2, and QPF$PSB3 as input. Modify QPF#PSB as necessary to match any changes that you made to the Stage1 SYSGEN source and where noted to match your data set names.

4. Build the message format service (MFS) format for use with the QPF Test Application MPP. Member QPF#MFS of the MAQCNTL library contains a sample MFSGEN job stream. This job uses MAQSAMP member QPFMFS as input.

   **Note**
   
   If any of the 3270 models that are displayed in QPFMFS are not defined to your IMS system, comment out the appropriate DEV statement and the UNSTACK statement that immediately follows the DEV statement. For example, if Model 4 is not defined to your IMS, comment out or remove the following statements:
   
   ```
   DEV TYPE=3270-A04,FEAT=IGNORE,SYSMSG=R23003
   UNSTACK,KEEP
   ```

5. Assemble and link-edit the routine that is used by the QPF Test Applications. Member QPF#WTOR of the MAQCNTL library contains the assembly/link-edit JCL. This job will create a load module that is referenced by QPF#COMP. The library in the SYSMOD DD statement in this job must also be used in QPF#COMP.

6. Compile and link-edit the QPF Test Applications. Member QPF#COMP of the MAQCNTL library contains the compile JCL. This job will use MAQSAMP members QPFMPP and QPFBMP to compile the MPP and both of the BMPs. Update the JCL according to the comments within the member.

   **Note**
If you are using the language environment (LE) in your IMS system, the LE library must be higher than other language libraries (COBOL and so forth) in the MPP/BMP STEPLIB concatenation.

The QPF Test Applications will be active the next time that you bring up your IMS system. For information about using the QPF Test Applications, see the Message Advisor for IMS User Guide.

Installing the Message Advisor Server

This section describes the steps that are required to install the Message Advisor Server.

1. Modify the Message Advisor Server JCL that is located in member QMR#ST RT of the MAQCNTL library.
   a. Change the PARM to match the Message Advisor Server name that you specified when you set the Message Advisor options.
      For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
   b. Change the STEPLIB DD to use the APF-authorized library that contains the Message Advisor modules.
   c. Change the QMROPTS DD to use the library that contains the options module.
2. Start the Message Advisor Server.
   a. After completing the changes from Step 1 (see page 212) in QMR#STRT, perform either of the following tasks:
      • Submit the job to run on the same MVS system as your IMS system
      • Place the Message Advisor Server JCL in PROCLIB and run the Message Advisor Server as an MVS-started task
   b. Start the Message Advisor Server on the same CPU that is executing your IMS system. See member QMR#STRT of the MAQCNTL library for sample JCL.
   c. When the Message Advisor Server is functional, an outstanding WTOR will display the Message Advisor title that you specified when you set the Message Advisor options.
      For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
      If the Message Advisor Server is ready to accept commands, message BMC43000I will be in the outstanding WTOR. If you receive message BMC43990I, check for previous VTAM error messages.

Bringing up your IMS system

To confirm that Message Advisor has been properly installed, perform the following steps:
1. Ensure that the IMSID of your system matches the IMSID that is specified in the QMRUOPT0 options module that you created when you set the Message Advisor options.
2. Confirm that you receive the following messages, where `imsid` is your IMSID:
   - BMC43772 Message Advisor INITIALIZATION COMPLETE `imsid`
   - BMC43712I Message Advisor CHECKPOINT TRACKING ACTIVE `imsid`
   If you do not receive the messages, you must concatenate the APF-authorized library again, and then reset the Message Advisor options. For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
3. To confirm that the QPF component has been properly installed, repeat Step 1 (see page 212) and Step 2 (see page 213).
4. Confirm that you receive the following QPF messages, where `imsid` is your IMSID:
   - BMC43002I QPF PRODUCT LEVEL vv.r.mmm.ll mm/dd/yyyy INITIALIZING FOR IMS `imsid`
   - BMC43157I QPF IS NOW ACTIVE `imsid`
   If QPF is not properly installed, message BMC43157I will indicate that QPF is inactive or you will receive the following messages:
     - BMC43152E QPF QPFOPTS MEMBER NOT FOUND IN PROC LIB
     - BMC43169A QPF FOR IMSID=`imsid` - INVALID QPF OPTIONS - REPLY RETRY OR IGNORE

Verifying Message Advisor installation

This section describes the procedures for testing your installation of Message Advisor.

Verifying Message Advisor installation consists of the following Installation Verification Procedure (IVP) tasks:

- **Performing the batch IVP for Message Advisor (see page 214)**
  This IVP task determines whether the Message Advisor Server routines will function with the targeted IMS systems.
- **Performing the online IVP for Message Advisor (see page 219)**
  This IVP task determines whether the CLIST and VTAM definitions, including the LU 6.2 connect between TSO and the Message Advisor Server, are properly installed and functioning.
- **Performing the IVP for QPF (see page 223)**
  If you installed the Message Advisor QPF component, this IVP task confirms that QPF has been installed properly.
  The QPF_OPTIONS command set that was activated during QPF installation provides a limited amount of queue overflow protection by preventing an IMS shutdown if a queue overflow tries to occur. You will be able to provide maximum protection for your message queues when you fully define the QPF_OPTIONS command set.
  For detailed instructions about defining the QPF_OPTIONS command set and activating it in your IMS system, see the *Message Advisor for IMS User Guide*. 

BMC System Administration for IMS, version 2.7.00
Performing the batch IVP for Message Advisor

This section describes the steps that are required to verify that the Message Advisor Server routines will function with the targeted IMS systems.

**Note**

For a shared queues (SQ) environment, ensure that you have a valid SQ IMSID.

1. Ensure that the IMS system that is defined in your customization parameter is up.
   The IMSID of your system must match the IMSID that is specified in options module QMRUOPT0, which you created when you set the Message Advisor options. For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
   If Message Advisor is properly installed in your IMS system, you will receive the following message:
   BMC43712I Message Advisor CHECKPOINT TRACKING ACTIVE
   If this message does not appear, you must again concatenate the APF-authorized library.

2. Update the IVP JCL.
   a. Select member QMR#IVP1 of the MAQCNTL library. The following figure shows the sample JCL that this member contains:

   ```plaintext
   BROWSE -- bmcnode.CNTL(QMR#IVP1) ----------- LINE 00000000 COL 001 080
   COMMAND ===>                                           SCROLL ===>PAGE
   **************************** TOP OF DATA ****************************
   //QMR#IVP1 JOB (ACCT),'MAQ DISPLAY ',REGION=4096K  <== MODIFY
   //*-------------------------------------------------------------------*
   //*                                                                   *
   //*  THIS JCL IS SUBMITTED TO TEST THE Message Advisor BATCH SERVER   *
   //*  MAKE THE FOLLOWING CHANGES                                      *
   //*     1. CHANGE QMRP     IN THE PARM TO YOUR SERVER_NAME            *
   //*     2. CHANGE STEPLIB TO YOUR APF-AUTHORIZED LIBRARY              *
   //*     2. CHANGE QMROPTS TO YOUR OPTIONS LIBRARY                     *
   //*     3. CHANGE IMSA TO YOUR IMSID                                  *
   //*-------------------------------------------------------------------*
   //DISPLAY  EXEC PGM=QMRCTL00,PARM='QMRP ,BATCH'  <== MODIFY
   //STEPLIB  DD  DISP=SHR,DSN=bmcnode.LOAD              <== MODIFY
   //QMROPTS  DD  DISP=SHR,DSN=bmcnode.LOAD              <== MODIFY
   //SYSPRINT DD  SYSOUT=*                                      
   //SYSDUMP DD  SYSOUT=*                                      
   //SYSSIN    DD  *                                          
   *     QMR#IMP2     TEST THE DISPLAY FEATURE
   DISPLAY  IMSID=IMSA,TYPE=STATISTICS ;  <== CHANGE TO YOUR IMSID
   END
   DISPLAY  IMSID=IMSA, ;  <== CHANGE TO YOUR IMSID
   TYPE=DEST_QUEUES,
   ```
b. Change the PARM parameter to match the Message Advisor Server name that you specified when you set the Message Advisor options. For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).

c. Change the STEPLIB DD to use the APF-authorized library that contains the Message Advisor modules.

d. Change the QMROPTS DD to use the library that contains the options module.

e. Change the IMSID to the IMSID that you specified when you set the Message Advisor options.

⚠️ **Note**

For shared queues verification, ensure that the IMSID is an IMS that is participating in a shared queues environment.

3. Submit the job and verify the job output.

   a. Submit the job to run on the same MVS system as your IMS system.

   b. Verify that the job completed with a condition code of zero or four. A condition code of zero indicates that the job completed successfully and that there are messages in the queue. A condition code of four indicates that the job completed successfully but that there are no messages in the queue.

   If you receive a condition code other than zero or four, review the output for accompanying error messages. Sample output from IVP JCL for batch processing of the Message Advisor QMR component (see page 215) shows sample output for the Message Advisor QMR component and Sample output from IVP JCL for batch processing of Message Advisor in a shared queues environment (see page 217) shows sample output for the Message Advisor QMR component in a shared queues environment.

   c. Review the output that contains message queue statistics and a report on messages that are queued to the master terminal, if any were queued. The following figure shows sample output for the Message Advisor QMR component and Sample output from IVP JCL for batch processing of Message Advisor in a shared queues environment (see page 217) shows sample output for the Message Advisor QMR component in a shared queues environment. The following figure shows a sample output report that was generated from IVP JCL for batch processing of the Message Advisor QMR component:
Sample output from IVP JCL for batch processing of the Message Advisor QMR component

```plaintext
DISPLAY IMSID=IMSA,TYPE=STATISTICS
END
DISPLAY IMSID=IMSA,
    TYPE=DEST_QUEUES,
    DESTINATION=MASTER
BMC43072I INPUT COMMANDS ACCEPTED, EXECUTION BEGINS
BMC43077I DISPLAY IN PROGRESS FOR RIHCLE (TASK 3)
>>>DISPLAY IMSID=IMSA,TYPE=STATISTICS
>>>END
Message Advisor V1.0.02 - Server ID QMRP          01.146 13.29.25

DISPLAY Statistics Information for IMSID IMSA

Queue utilization: Short  1% Long 1%
Top Ten Destination Message Queues
ACCTRPT . . . . . . . . . . . . . . : 32
APPGM . . . . . . . . . . . . . . : 11
LTRM3270. . . . . . . . . . . . . . : 11
PART . . . . . . . . . . . . . . : 7
ADDPART . . . . . . . . . . . . . . : 7
PMASTER . . . . . . . . . . . . . . : 5
SMASTER . . . . . . . . . . . . . . : 5
LTRM3278. . . . . . . . . . . . . . : 5
SLU$2002. . . . . . . . . . . . . . : 4
MASTER . . . . . . . . . . . . . . : 2

Total messages for CNTs . . . . . . : 75
Total messages for SMBs . . . . . : 14
Total messages for TPnames . . . . : 0
Total messages for TPIPES . . . . : 0

Number of LTERMs (CNTs) . . . . . : 250
Number of transactions (SMBs) . . : 71
Number of TPnames(QABs/TIBs) . . : 0
Number of TPIPES(YQABs/YTIBs) . : 0

Number of main memory queue buffers : 50
Main memory queue buffer size . . . : 6,720
Number of errors . . . . . . . . . : 0
Number of messages cancelled . . . : 62
Current SHMSG lrecl size . . . . . : 336
Current LGMSG lrecl size . . . . . : 3,360
Maximum length of message prefix . . . : 376
Size of basic prefix . . . . . . : 20
Size of full extension . . . . . : 64
Size of short prefix extension . . : 4
Size of MSC segment item . . . . : 64
Size of RACF segment item . . . : 20
Size of LU6 segment item . . . : 22
# records larger than SHMSG lrecl . : 0
```
The following figure shows a sample output report that was generated from IVP JCL for batch processing of Message Advisor in a shared queues environment:

Sample output from IVP JCL for batch processing of Message Advisor in a shared queues environment

```
DISPLAY        IMSID=GCB6,TYPE=STATISTICS
END

DISPLAY        IMSID=GCB6,TYPE=DEST_QUEUES,DESTYPE=ALL,
DESTINATION=SMASTER
END

BMC43072I INPUT COMMANDS ACCEPTED, EXECUTION BEGINS
BMC43077I DISPLAY IN PROGRESS FOR RIHGCB2 (TASK 2)

>>DISPLAY        IMSID=GCB6,TYPE=STATISTICS
>>END

Message Advisor V1.0.02 - Server ID @@@@@@@@      01.135 15.54.35

DISPLAY Statistics Information for IMSID GCB6

Queue utilization: Ovf 59% Primary 47%

Queue utilization: Ovf 59% Primary 47%
Top Ten Destination Message Queues
  Sequenced by space used for FIC recs
DEST152 .......................... : 986
DESTB ............................ : 675
DESTZ0 ........................... : 792
DESTZC ........................... : 626
DESTBP ............................ : 530
DESTO ............................. : 381
DEST3 ............................. : 372
DEST136 ........................... : 360
DESTZM ........................... : 308
DESTZA ............................ : 257
```
Total messages for CNTs: 7,677
Total messages for SMBs: 430
Total messages for TPnames: 4
Total messages for TPIPES: 0

Number of LTERMs (CNTs): 58
Number of transactions (SMBs): 4
Number of TPnames (QABs/TIBs): 2
Number of TPIPES (YQABs/YTIBs): 0

Number of main memory queue buffers: 500
Main memory queue buffer size: 6,720
Number of errors: 0
Number of messages cancelled: 63

Current SHMSG lrecl size: 296
Current LGMSG lrecl size: 6,680
Maximum length of message prefix: 940
Size of basic prefix: 64
Size of full extension: 64
Size of short prefix extension: 4
Size of MSC segment item: 92
Size of RACF segment item: 20
Size of LU6 segment item: 22

--------- PRIMARY STRUCTURE ---------
Structure element size: 512
Maximum number of struct elements: 34,847
Number of struct elements in use: 16,505
Maximum number of struct entries: 34,847
Number of struct entries in use: 5,421

--------- OVERFLOW STRUCTURE ---------
Max Overflow struct elements: 34,847
Number of Overflow elements in use: 20,775
Max Overflow struct entries: 34,847
Number of Overflow entries in use: 5,089

IMS RESTART DATE AND TIME: 01/135-15:46:04.2
BMC43076I DISPLAY FOR RIHGCB2 (TASK 2) IMS(GCB6) ENDED, RC=00
BMC43077I DISPLAY IN PROGRESS FOR RIHGCB2 (TASK 2)

>> DISPLAY IMSID=GCB6, TYPE=DEST_QUEUES, DESTYPE=ALL,
>> DESTINATION=SMASTER

DISPLAY Analyzer Report for IMSID GCB6
TYPE DESTINATION MSGS RECS SEGSGSHMSG %LGMSG PSB/LU/REGI
TRAN/REG
CNT SMASTER 29 29 92 .00 .29

DISPLAY Analyzer Report for IMSID GCB6
>> GLOBAL QUEUES <<
TYPE DESTINATION MSGS RECS SEGSGOVF %PRI PSBNAME/LU
LTRM5 SMASTER 27 27 54 .14
Performing the online IVP for Message Advisor

This section describes the steps that are required to verify that the CLIST and VTAM definitions, including the LU 6.2 connect between TSO and the Message Advisor Server, are properly installed and functioning.

To complete the online IVP for Message Advisor, perform the following steps:

1. Ensure that the IMS system that is defined in your options module is up.
   The IMSID of your system must match the IMSID that is specified in options module QMRUOPT0, which you created when you set the Message Advisor options. For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
   If Message Advisor is properly installed in your IMS system, you will receive the following message:
   BMC43712I Message Advisor CHECKPOINT TRACKING ACTIVE
   If this message does not appear, you must again concatenate the APF-authorized library.

2. Vary the active Message Advisor APPLIDs.
   Issue VTAM commands to vary the active APPLIDs for the Message Advisor Server and user sessions. The VARY commands must recognize the member that you previously created to hold the VTAM APPLID statements.
   The members that hold the VTAM APPLID statements are created when you add the Message Advisor VTAM specifications to your SYS1.VTAMLST data set or its equivalent.

   Note
   If you have a multiple-CPU system, be sure to issue the VARY commands on the appropriate system.

3. Select the Message Advisor ISPF menu.
   a. From the ISPF/PDF Primary Option Menu, select the Message Advisor option, or type TSO %QMRCLIST on the Command line and press Enter.
   b. The Message Advisor banner panel is displayed. Press Enter to display the Message Advisor Primary Menu.

   Message Advisor Primary Menu

       File   Session   Display   Help
       ______________________________________________________
       ___
3. **b.** 4.

Message Advisor - Primary Menu  Product Level: V1.04

Select one of the following. Then press Enter.

1. Build and execute Message Advisor requests
   Request library bmcnode.REQUEST

2. Display and/or dequeue specific IMS messages
3. Display statistics for the IMS messages queues
4. List IMS log/checkpoint history
5. Customize Server and IMS options
6. Execute Message Advisor and IMS commands
7. BMC Software Product Authorization by CPU ID
8. Queue Protection Facility
9. Analyzer Display for Shared Queues

IMSID . . . . Q22P+ (for options 2, 3, 4, 6, 8, 9)
Server name . . QMRP+ (all options)
'+' following an entry field indicates that the PROMPT action is available.
(c) Copyright 2001 BMC Software, Inc. as an unpublished licensed work.
All rights reserved.

4. Type **2** in the choice entry field.

5. Type the IMSID for which you want to display destination information in the **IMSID** field and press **Enter**.

⚠️ **Note**

For shared queues verification, ensure that the IMSID is an IMS that is participating in a shared queues environment.

The Destination Selection pop-up panel is displayed.

⚠️ **Note**

If you have a different VTAM APPLID than the default MADV, the VTAM Session pop-up panel will be displayed before the Destination Selection pop-up panel is displayed. Specify the appropriate VTAM APPLID and press **Enter**.

**Destination Selection pop-up panel**

File  Session  Display  Help

---

Destination Selection - Non-shared Queues
6. Define the destination selection criteria.
   a. Verify that the IMSID that is displayed in the IMSID field is accurate.
   b. Type 1 in the **Destination type** field.
   c. If you want to sort the output, type the option for the kind of sort that you want
      Message Advisor to perform in the Sort by field.
   d. If you want to sort the output, type a limit for the number of destinations that you want
      Message Advisor to display in the Limit sort display to field.

   ![Note]
   
   A limit is required if you want to sort the output. Sort performance depends on the number of destinations that you specify. The smaller the number of destinations that you specify, the faster Message Advisor will perform the sort.

   e. Type a destination that is valid for your site in the Dest field, or leave the field blank if you want to display all destinations for the IMSID.
      The following masking is allowed in the Dest field: ? replaces one character in a multi-character string; * replaces the rest of the string.
      If you type an LU name in the LUname field, you must also enter a destination.
      Furthermore, an LUname entry is only valid for TPNAME destinations.
   f. Type 2 in the **Format** option field.
      Selecting this format option causes a hexadecimal dump of the prefix and message text.
g. If you want to display only queues that are being created by a specific region, type a dependent region name in the **Region** field.

The following masking is allowed in the **Region** field: ? replaces one character in a multi-character string; * replaces the rest of the string.

h. Press **Enter**.

The **Destination List pop-up panel** is displayed.

**Destination List pop-up panel**

```
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination List</td>
</tr>
<tr>
<td>Type one or more action codes. Then press Enter.</td>
</tr>
<tr>
<td>A S=Display messages D=Dequeue messages Row 00001 of 00063</td>
</tr>
<tr>
<td>c F=Force messages                                                    More:</td>
</tr>
<tr>
<td>+ &gt;</td>
</tr>
<tr>
<td>RegID</td>
</tr>
<tr>
<td>_ MSNAME MSC12 15 15 16 .01% .00%</td>
</tr>
<tr>
<td>_ CNT-V CAT 2,001 2,001 2,001 .00% 5.55%</td>
</tr>
<tr>
<td>_ CNT-V TEMPD002 1 1 1 .01% .00% LSGTEMPQ 1</td>
</tr>
<tr>
<td>_ CNT-V TEMPD003 1 1 1 .01% .00% LSGTEMPQ 1</td>
</tr>
<tr>
<td>_ CNT-V TEMPD004 1 1 1 .01% .00% LSGTEMPQ 1</td>
</tr>
<tr>
<td>_ SMB DSPINV 5 5 5 .00% .01% DFSSAM03</td>
</tr>
<tr>
<td>_ TPNAME DFSCMD 15 15 65 .00% .04% PVCSHOUA</td>
</tr>
<tr>
<td>_ TPNAME DFSASYNC 737 737 2,334 .00% 2.04% PVCSHOUA</td>
</tr>
<tr>
<td>_ TPNAME NAME_200 &gt; 2 2 2 .00% .01% R51ML62</td>
</tr>
<tr>
<td>_ TPNAME NAME_100 &gt; 2 2 2 .00% .01% R51ML62</td>
</tr>
<tr>
<td>_ TPNAME NAME_300 &gt; 2 2 2 .00% .01% R51ML62</td>
</tr>
</tbody>
</table>
```
Review the list of destinations.
The displayed messages confirm that Message Advisor is properly installed.

Note
If you select a temporary queue for display, the Tran/Reg and RegID values will also be displayed at the top of the Message List and Message Display panels.

Performing the IVP for QPF

This section describes the steps that are required to verify that the Message Advisor QPF component has been properly installed.

QPF should have been activated during the installation process. This IVP submits a QPF_OPTIONS request to list the QPF options that were initially set when QPF was activated.

To complete the IVP for QPF, perform the following steps:

1. Ensure that the IMS system that is defined in the Message Advisor QMR component options module is up.
   a. Verify that the IMSID of your system matches the IMSID that is specified in the QMRUOPT0 options module, which you created when you set the Message Advisor options. For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
   b. Verify that you receive the following message, where `imsid` is your IMSID:

   `BMC43157I QPF IS NOW ACTIVE imsid`

   If this message does not appear, review your installation steps for a possible reason. A common reason for this message not being issued is that the APF-authorized library has been omitted.

2. Update the QPF IVP options command set.
   a. Select member QPF@IVP2 from the MAQSAMP library.
      This member, shown in the following figure, contains one command set with two requests. The first request sets the QPF options. The second request lists the options that the IMS is currently using.

   **QPF command set for the QPF IVP**

   ```plaintext
   QPF_OPTIONS IMSID-?,TYPE=SET,ACTIVE=YES,MAX_REGION=3M, <= CHANGE TO YOUR IMSID
   MONITOR_PHASE
   PROTECT_PHASE
   ```
b. Change IMSID to match the IMS system that you specified when you set the Message Advisor options.

3. Submit a batch job to execute the command set.
   a. Select member QMR#BJCL in the MAQCNTL data set (or use existing Message Advisor Batch Server JCL).
   b. Change the PARM parameter to match the Message Advisor Server name that you specified when you set the Message Advisor options. For information about setting the Message Advisor options, see Setting the Message Advisor options (see page 193).
   c. Change the STEPLIB DD to use the APF-authorized library that contains the Message Advisor modules.
   d. Change the QMROPTS DD to use the library that contains the options module.
   e. Point the SYSIN DD statement to the modified QPF@IVP2.

4. Submit the job and verify the output.
   a. Submit the job to run on the same MVS system as your IMS system.
   b. The job output should list the options that were set before you added your userID and confirm that the options were changed.

Sample output from IVP JCL for batch processing of QPF (see page 224) shows a sample output report.

---

**Note**

When THRESHOLD% and RESET% values are not specified for the three phases, QPF calculates the following default values:

- For the Monitor phase, the THRESHOLD% is the IMS QTL value and the RESET% is the Monitor phase THRESHOLD%.
- For the Protect phase, the THRESHOLD% is the IMS QTU value and the RESET% is the Monitor phase THRESHOLD%.
- For the Overflow phase, the THRESHOLD% is 99 and the RESET% is the Overflow phase THRESHOLD% minus 1.

The following figure shows a sample output report that was generated from IVP JCL for batch processing of QPF.

**Sample output from IVP JCL for batch processing of QPF**

```
QPF_OPTIONS IMSID=VJD9,TYPE=SET,ACTIVE=YES,MAX_REGION=3M
MONITOR_PHASE
PROTECT_PHASE
```
OVERFLOW_PHASE
END

QPF_LIST IMSID=VJD7,TYPE=OPTIONS
END

BMC43072I INPUT COMMANDS ACCEPTED, EXECUTION BEGINS
BMC43077I QPF_OPTIONS IN PROGRESS FOR RIHVJD (TASK 2)
>>>QPF_OPTIONS IMSID=VJD9,TYPE=SET,ACTIVE=YES,MAX_REGION=3145728
>>> MONITOR_PHASE
>>> PROTECT_PHASE
>>> OVERFLOW_PHASE
>>>END

BMC43140I MESSAGE ADVISOR QPF HIPERASSIST IS NOW ACTIVE, IMSID=VJD9
BMC43157I MESSAGE ADVISOR QPF OVERFLOW PROTECTION IS NOW ACTIVE, IMSID=VJD9
BMC43076I QPF_OPTIONS FOR RIHVJD (TASK 2) IMS(VJD9) ENDED, RC=00
BMC43077I QPF_LIST IN PROGRESS FOR RIHVJD (TASK 2)
>>>QPF_LIST IMSID=VJD9,TYPE=OPTIONS
>>>END

QPF Options - General

<table>
<thead>
<tr>
<th>IMSID</th>
<th>VJD9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overflow protection.</td>
<td>YES</td>
</tr>
<tr>
<td>Hiperassist.</td>
<td>YES</td>
</tr>
<tr>
<td>Hiperspace usage.</td>
<td>ESO</td>
</tr>
<tr>
<td>Maximum ASM% usage</td>
<td></td>
</tr>
<tr>
<td>Maximum hiper pages</td>
<td>1024K</td>
</tr>
<tr>
<td>Move-page facility</td>
<td>YES</td>
</tr>
<tr>
<td>Maximum region</td>
<td>3072K</td>
</tr>
<tr>
<td>Dump</td>
<td>ON_ERROR</td>
</tr>
<tr>
<td>Trace</td>
<td>INTERNAL</td>
</tr>
<tr>
<td>Trace table size</td>
<td>83648</td>
</tr>
<tr>
<td>Log code</td>
<td>EF</td>
</tr>
<tr>
<td>Notify</td>
<td>WTO</td>
</tr>
</tbody>
</table>

QPF Options - Phases

<table>
<thead>
<tr>
<th>Threshold% - phase starts at</th>
<th>Monitor</th>
<th>Protect</th>
<th>Overflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>60%</td>
<td>75%</td>
<td>99%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reset% - phase stops at</th>
<th>Monitor</th>
<th>Protect</th>
<th>Overflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>60%</td>
<td>60%</td>
<td>98%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reset time - delay in minutes</th>
<th>Monitor</th>
<th>Protect</th>
<th>Overflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

QPF Options - General

<table>
<thead>
<tr>
<th>IMSID</th>
<th>VJD9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overflow protection.</td>
<td>YES</td>
</tr>
<tr>
<td>Hiperassist.</td>
<td>YES</td>
</tr>
<tr>
<td>Hiperspace usage.</td>
<td>ESO</td>
</tr>
<tr>
<td>Maximum ASM% usage</td>
<td></td>
</tr>
<tr>
<td>Maximum hiper pages</td>
<td>1024K</td>
</tr>
<tr>
<td>Move-page facility</td>
<td>YES</td>
</tr>
<tr>
<td>Maximum region</td>
<td>3072K</td>
</tr>
<tr>
<td>Dump</td>
<td>ON_ERROR</td>
</tr>
<tr>
<td>Trace</td>
<td>INTERNAL</td>
</tr>
<tr>
<td>Trace table size</td>
<td>83648</td>
</tr>
<tr>
<td>Log code</td>
<td>EF</td>
</tr>
</tbody>
</table>
Notify . . . . . . . : WTO

QPF Options - Phases
Threshold% - phase starts at . . . . . : 60%  75%  99%
Reset% - phase stops at . . . . . . . : 60%  60%  98%
Reset time - delay in minutes . . . . : 15   1   0

QPF Options - General
IMSID . . . . . . . : VJD9
Overflow protection . : YES
Hiperassist . . . . . : YES
Hiperspace usage . . : ESO
Maximum ASM% usage . : 
Maximum hiper pages  : 1024K
Move-page facility . : YES
Maximum region . . . : 3072K

Dump . . . . . . . . : ON_ERROR
Trace . . . . . . . . : INTERNAL
Trace table size . . : 83648
Log code . . . . . . : EF
Notify . . . . . . . : WTO

QPF Options - Phases
Threshold% - phase starts at . . . . . : 60%  75%  99%
Reset% - phase stops at . . . . . . . : 60%  60%  98%
Reset time - delay in minutes . . . . : 15  1  0
ITASKS started for this phase . . . . : 2  1  0
WTO . . . . . . . . . . . . . . . . : YES  YES  YES
WTO descriptors . . . . . . . . . . . : X'0200'  X'0200'  X'0200'
WTO routing codes . . . . . . . . . : X'4200'  X'4200'  X'4200'

Notify% - %change for next message . . :
Notify interval - in minutes . . . . . :
Notify recipients . . . . . . . . . . :

Mode (protect) . . . : LOG,WARN,PROCESS,REPEAT
Actions (overflow) . : INWAIT
System wait . . . . : AT_SHUTDOWN

Monitor auto command :
Protect auto command :
Overflow auto command :

QPF Options - Enforce - None
QPF Options - Process - None
QPF Options - Unload - None

BMC43076I QPF_LIST FOR RIHVJD (TASK 2) IMS(VJD9) ENDED, RC=00
Customizing the console

This section describes tasks for customizing the console. Customization refers to tasks that you perform outside of the Installation System to complete product implementation. The following topics are covered in this section:

- Overview of customizing the GUI Console (see page 227)
- Console customization worksheet (see page 227)
- Customizing the UIM server console (see page 228)
- Launching and exiting the console (see page 229)
- Managing UIM server clients (see page 230)
- Setting up connections (see page 231)

Overview of customizing the GUI Console

The console is the graphical user interface (GUI).

The console runs on a client workstation under the Microsoft Windows operating system and communicates with the UIM server through TCP/IP technology.

The following BMC system administration products for IMS offer functions that are console-enabled:

- BMC System Administration for IMS
- BMC System Communication for IMS
- Energizer for IMS Connect

Console customization worksheet

The following table is a worksheet that lists the steps you must complete to customize the console:

<table>
<thead>
<tr>
<th>Step</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the console.</td>
<td>Customizing the UIM server console (see page 228)</td>
</tr>
<tr>
<td>2. Launch and exit the console.</td>
<td>Launching and exiting the console (see page 229)</td>
</tr>
<tr>
<td>3. Manage UIM server clients.</td>
<td>Managing UIM server clients (see page 230)</td>
</tr>
<tr>
<td>4. Set up connections.</td>
<td>Setting up connections (see page 231)</td>
</tr>
</tbody>
</table>
Customizing the UIM server console

After the UIM server is installed and running, you can install, customize, and update the console.

The UIM server downloads the required code to the console computer. Depending on your user privileges on that computer, you can install the console as follows:

- If you have administrator rights, you can install one instance of the console to be shared by all users of that computer. Tracing and logging are fully supported in this case. The default installation location is `C:/Program Files/BMC Software/Database Management Console`.
- If you do not have administrator rights, you can install a single instance of the console for your use. However, tracing and logging might not work. The default installation location is `C:/Documents and Settings/user/My Documents/BMC Software/Database Management Console`.

Installing the console

Use the following procedure to install the console on a personal computer.

Before you begin

You will need:

- The name of the host computer on which the UIM server is running
- The UIM server’s port number
- Access to a supported web browser

If you do not know the host name and port number, consult your system administrator.

To install the console

1. From your web browser, enter the URL for the UIM server on the mainframe.
   For example, enter `http://uimServerHostName:uimPortNumber/dna/index.html`, replacing the variables with your information.
2. On the resulting web page, click Install Local Client.
3. Based on the browser that you are using, either open the file from its current location, or save the file to your hard drive and then run the program:
   - If you are using Internet Explorer, perform the following steps:
     a. In the File Download dialog box, select Run this program from its current location, and click OK.
     b. If the Security Warning dialog box is displayed, click Yes.
   - If you are using Mozilla Firefox or a similar browser, perform the following steps:
     a. In the Save As dialog box, select a location in which to save the installation file, and click Save.
     b. The .exe file is downloaded.
     c. Browse to the saved file, and double-click it.
4. Enter the requested information in the BMC Database Management Wizard.
5. On the last page of the wizard, select **Launch the Database Management Console**.
6. Click **Finish**.
   The BMC Database Management Console starts.

### Updating the console

When you launch the console, the files on your personal computer (local client) are compared to the file residing on the UIM server.

If a change in the installed products has occurred, the console is updated automatically.

⚠️ **Note**

If the program that installs the console on the UIM server is updated, you must enter the URL for the UIM server on the mainframe to update the console. For more information, see [Installing the console](#) (see page 228).

### Uninstalling the console

Use the following procedure if you need to remove the console from your personal computer.

**To uninstall the console**

1. In Microsoft Windows, open the Control Panel.
   For more information, see the documentation for your version of Windows.
2. In the Control Panel window, click **Add/Remove Programs**.
3. Select and uninstall **BMC Database Management Console (user)**.
   The value of `user` is `Admin` if the console was installed by an administrator; otherwise, the value is the relevant user name.

### Launching and exiting the console

The console uses z/OS authentication.

When you launch the console, you must provide a valid SAF user ID and password. The security administrator for your site manages the SAF account information for users.
To launch the console

1. From the Start menu, select All Programs > BMC Software > Database Management Console.

The login dialog box is displayed.

To exit the console

1. From the File menu, select Exit.

2. On the Quit? dialog box, click Yes.

Managing UIM server clients

When you launch the console, you can manage your UIM server clients from the login dialog box.
To manage the UIM server clients

1. From the Start menu, select All Programs > BMC Software > Database Management Console.
   The BMC Database Management Console login dialog box is displayed.
2. Click the (More) button to the right of the Host box.
   The Manage UIM Server Clients dialog box is displayed.

   Manage UIM Server Clients dialog box

3. Take the appropriate actions to manage your host list:
   - To add a host, click Add button and complete the fields in the Details area.
   - To edit a host, select it in the host list, click Edit and change the fields in the Details area as needed.
   - To delete a host, select it in the host list, and click Delete.
   - To define a host to display as the default host when logging into the console, click the check box next to the host name.

Setting up connections

When you launch the console, you must define at least one host connection. After defining a host connection, you can work with resources on that host. The connection definition remains available whenever you start the console and log on. The names of all defined connections are listed in the Connections folder on the Main tab of the Navigation window.

Overview of the Enterprise List and personal connections

Host connections for individual users are managed separately from host connections for the entire enterprise.

This separation makes it easier to isolate activities in different environments (such as testing systems versus production systems or application systems versus other application systems).
The console uses a shared Enterprise List of connections. This list resides on the UIM server. Users who have the appropriate security authority can add, delete, and edit connection information in the Enterprise List. When any user launches the console, the Enterprise List identifies the host connections that are defined.

Each user has a personal list of connections. You can define a connection in your personal list manually by entering connection information (such as the host name and port number). You can also add connections to your personal list by selecting predefined connections from the Enterprise List. After you define a host connection in your personal list, that connection definition remains available whenever you start the console and log on.

Managing the Enterprise List

If you have the appropriate authority, use the following procedure to add, edit, or delete connections in the shared Enterprise List on the UIM server.

To manage the Enterprise List

1. On the Main tab of the Navigation window, right-click the Connections folder and select **Manage Host Connections in the Enterprise List**.
   The Manage Enterprise Connections dialog box is displayed.
2. Add, edit, or delete a connection as follows:

<table>
<thead>
<tr>
<th>To</th>
<th>Perform these steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a connection</td>
<td>a. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Enter the connection information in the <strong>Details</strong> area.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Done</strong>.</td>
</tr>
<tr>
<td>Edit a connection</td>
<td>a. Select the connection, and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Change the connection information in the <strong>Details</strong> area.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Done</strong>.</td>
</tr>
<tr>
<td>Delete a connection</td>
<td>a. Select the connection.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
3. Click **OK** to apply your changes to the shared Enterprise List and close the dialog box.

Using the Add Host Connection command

To define a single connection quickly, use the **Add Host Connection** command.

Use this method to create a connection definition when you know the required connection information, such as host and port.

To add a connection

1. On the Main tab of the Navigation window, right-click the Connections folder and click **Add Host Connection**.
The Define Connection dialog box is displayed.

2. In the **Host** box, enter the name of the host.

3. In the **Port** box, enter the UIM port number.

   The value in the **Display Name** field is generated automatically from the host name and the port number.

4. *(optional)* In the **Description** box, enter a descriptive name for the connection.

5. In the **Login Information** area, select whether to connect by using console credentials or with credentials that you specify.

   ![Note](image)

   **Note**

   Console credentials are the user name and password that you used to log on to the console. If you select **Connect using these credentials**, you must enter a user name and password. If necessary, you can also enter the account and group to which the user name belongs.

6. *(optional)* To connect automatically whenever the console starts, select **Autoconnect at console start**.

7. Click **OK**.

   The new host connection is displayed in the **Connections** folder on the Main tab of the Navigation window.

**To connect to a host**

1. On the Main tab in the Navigation window, right-click the host connection and click **Connect**.
   
   The Connect dialog box displays the connection information for the selected host.

2. In the **Login Information** area, select whether to connect by using console credentials or with credentials that you specify.

   ![Note](image)

   **Note**

   Console credentials are the user name and password that you used to log on to the console. If you select **Connect using these credentials**, you must enter a user name and password. If necessary, you can also enter the account and group to which the user name belongs.

3. *(optional)* To connect automatically whenever the console starts, select **Autoconnect at console start**.

4. Click **OK**.
Operating the UIM server

This section provides information about operating the UIM server. The following topics are covered:

- Overview of customizing the UIM server (see page 234)
- Operating the UIM server1 (see page 234)
- Merging multiple products into a single UIM server (see page 240)
- Creating a new UIM server (see page 244)
- Customizing the UIM server (see page 249)

Overview of customizing the UIM server

The UIM server resides on the mainframe and handles communication between the console and BMC console-enabled mainframe products and features.

Operating the UIM server1

You can control the operation of the UIM server through a web browser. If the UIM server is not running, you cannot run the console. From a web browser, you can start and stop the UIM server, view the active users, change the security authorization feature, and refresh the content of the UIM server. You can also change the status of the response logs and the internal trace.

Starting and stopping the UIM server

Before you start the console, the UIM server must be running.

If the UIM server is not running, you cannot run or install the console. In addition, you cannot access any UIM commands through a web browser.

To start and stop the UIM server, you must issue MVS operator commands on the host that the UIM server is installed on.

⚠️ Warning

To avoid data loss, notify active users when you must stop the UIM server.

To start the UIM server

Issue the following MVS operator command:

```
S uimServerName
```

`uimServerName` is the name of the UIM server started task.
To stop the UIM server

Issue the following MVS operator command:

\[ P \text{ uimServerName} \]

*uimServerName* is the name of the UIM server started task.

Verifying that the UIM server is running

You can verify whether the UIM server is running or not by reviewing the JESMSGLG SYSOUT file.

To verify that the UIM server is running

To verify that the UIM server is running, review the JESMSGLG SYSOUT file for the following messages:

- BMC340290I UIM server, Level v.r.mm mm,dd,yy, initialization complete!
- BMC340122I Ready for MVS Operator Commands

Accessing the BMC UIM server Commands web page

All UIM server operation tasks are performed from the BMC UIM server Commands web page.

The UIM server must be started before you can access this web page.

Authorization settings

Before you can access the BMC UIM server Commands web page, the variable ALLOW_NETCMD must be set in the UIM startup member.

For information about this variable, see the information about enabling the network browser command interface in your configuration documentation.

**ALLOW_NETCMD variable settings**

<table>
<thead>
<tr>
<th>ALLOW_NETCMD setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The BMC UIM server Commands web page is disabled.</td>
</tr>
<tr>
<td>YES</td>
<td>The BMC UIM server Commands web page is enabled.</td>
</tr>
<tr>
<td>AUTH</td>
<td>You must log into the console UIM server Logon web page to verify that you are allowed to access the BMC UIM server Commands web page. If the logon is successful, the user can display the BMC UIM server Commands web page.</td>
</tr>
</tbody>
</table>
If the AUTH setting has been set in the UIM startup member, and you are not authorized to access the BMC UIM server Commands web page, you will see the following message in your browser when you try to access the web page:

403 - Access to URN not allowed

If you see this message, you must follow the steps in To access the BMC UIM server Commands web page using authorization (see page 236).

To access the BMC UIM server Commands web page

From a supported web browser, enter the following URL for the BMC UIM server Commands web page:

http://uimServerHostName:uimPortNumber/htpcmd.html

The variables in the URL are defined as follows:

- uimServerHostName is the name of the host computer on which the UIM server is installed.
- uimPortNumber is the port number that is assigned to the UIM server. The default is 9999.

For example: http://syso:9999/htpcmd.html

To access the BMC UIM server Commands web page using authorization

1. From a supported web browser, enter the following URL for the console UIM server Logon web page:
   
   http://uimServerHostName:uimPortNumber/UIMLogon
   
   The variables in the URL are defined as follows:
   
   - uimServerHostName is the name of the host computer on which the UIM server is installed.
   - uimPortNumber is the port number that is assigned to the UIM server. The default is 9999.

   For example: http://syso:9999/UIMLogon

2. Enter your user ID and password.

3. (optional) Enter a group identification and account.

   Note
   
   You can change the password on the UIM host by entering a new password in the New Password field.

4. Click OK.
   
   The message Logon successful is displayed in your web browser. The authentication for the UIM server is stored in a cookie in your web browser.
5. Enter the following URL for the BMC UIM server Commands web page:
   http://UimServerHostName:uimPortNumber/htpcmd.html
6. To stop access to the BMC UIM server Commands web page, enter the following URL:
   http://UimServerHostName:uimPortNumber/UIMLogoff

Viewing active users

Active users are any users who are logged on to a console.

To view the names of active users

1. Access the BMC UIM server Commands web page as described in Accessing the BMC UIM server Commands web page (see page 235).
2. Click Display Active Users.
   The UIM server Active User Display page is displayed, and the names of the active users are listed on the page.
3. Return to the BMC UIM server Commands web page by clicking Back to UIM server Commands.

Changing the security authorization timeout feature temporarily

You can change the security authorization timeout feature temporarily for consoles that communicate with the UIM server.

The change will remain effective until the UIM server is stopped.

```
Note
Performing this task changes the timeout feature temporarily for all consoles that communicate with the UIM server.
```

To change the timeout feature temporarily

1. Access the BMC UIM server Commands web page as described in Accessing the BMC UIM server Commands web page (see page 235).
2. Click Display Active Users.
   The UIM server Active User Display page is displayed.
3. In the Inactivity Time Out box, type a value (in minutes or seconds) representing the amount of time that the console can remain inactive without timing out.
4. Choose a unit of time for the console timeout feature by selecting the option button for Seconds or Minutes.
5. Apply your changes by clicking Change.
6. Return to the BMC UIM server Commands web page by clicking Back to UIM server
   Commands.

Enabling or disabling the overall tracing option temporarily

You can enable or disable the overall tracing option temporarily for the UIM server.

The change remains effective until the UIM server is stopped or until you change it.

Trace data is written to the TRCLOGDD. To view trace data, review the contents of the
TRCLOGDD.

To enable or disable the overall tracing option temporarily

1. Access the BMC UIM server Commands web page as described in Accessing the BMC UIM
   server Commands web page (see page 235).
2. On the BMC HTTP Server Commands Web page, click Internal Trace – Display Trace Status
   /Modification.
   The Trace Indicator Status page is displayed. The status of the tracing option is shown in
   the Overall Trace Indicators section.
3. In the Overall Trace indicators section, select either Active or Inactive.
   • If the overall tracing option is disabled and you want to enable it, click Inactive in the
     Overall Trace column.
     Inactive changes to Active, indicating that the overall tracing option has been enabled
     for the UIM server.
   • If the overall tracing option is enabled and you want to disable it, click Active in the
     Overall Trace column.
     Active changes to Inactive, indicating that the overall tracing option has been disabled for
     the UIM server.
4. Return to the BMC HTTP Server Commands Web page by clicking Back to HTTP Server
   Commands.

Enabling or disabling specific tracing options temporarily

You can enable or disable specific tracing options temporarily for the UIM server.

The change remains effective until the UIM server is stopped or until you change it.

Trace data is written to the TRCLOGDD. To view trace data, review the contents of the
TRCLOGDD.

To enable or disable specific tracing options temporarily

1. Access the BMC UIM server Commands web page as described in Accessing the BMC UIM
   server Commands web page (see page 235).
2. On the BMC HTTP Server Commands Web page, click **Internal Trace – Display Trace Status**

The Trace Indicator Status page is displayed. The status of the tracing option is shown in
the Overall Trace Indicators section.

3. In the Overall Trace Indicators section, ensure that the tracing option is set to **Active**.
If the overall tracing option is set to Inactive, click **Inactive** in the Overall Trace column.
Inactive changes to Active, indicating that the overall tracing option has been enabled for the
UIM server.

![](Note)

**Note**

The overall trace option must be Active before you can enable or disable specific
tracing options.

4. In the Trace Components Indicators section, find the category for the specific tracing option
that you want to enable or disable:

   - Trace components
   - Trace actions

5. To enable or disable specific tracing options, perform one of the following tasks:

   - If tracing is disabled for a specific option and you want to enable it, click **Off** in the
     Status column.
     Off changes to On, indicating that tracing has been enabled for that option.

   - If tracing is enabled for a specific option and you want to disable it, click **On** in the
     Status column.
     On changes to Off, indicating that tracing has been disabled for that option.

6. Return to the BMC HTTP Server Commands Web page by clicking Back to HTTP Server

Commands.

**Refreshing the UIM server content**

You can refresh the content of the UIM server without shutting it down.

You may need to refresh the content of the UIM server when a new version is installed.

**To refresh UIM server content**

1. Access the BMC UIM server Commands web page as described in Accessing the BMC UIM
   server Commands web page (see page 235).

2. Click **Display/Refresh Contents Directory**.
   The MVS Content Index page is displayed.

3. On the MVS Content Index page, click **Refresh Content Index**.

4. Return to the BMC UIM server Commands web page by clicking Back to UIM server
   Commands.
Merging multiple products into a single UIM server

If you have a UIM server already installed on a z/OS image, and you install an additional product that uses the UIM server, you can merge the two UIM servers into a single UIM server and a single started task procedure.

If you install multiple IMS and DB2 products during the same Installation System session, the products will automatically share the UIM server that you specify.

If you have a UIM server already installed on a mainframe, and you install new products on the same mainframe, you must manually customize both products to share the same UIM server.

To merge IMS and DB2 products into sharing one UIM server, see the instructions in Sharing a Installation System server with DB2 and IMS products (see page 240).

To merge multiple IMS products into sharing one UIM server, see the instructions in Sharing UIM server with multiple IMS products (see page 243).

Sharing a Installation System server with DB2 and IMS products

If you have installed a Installation System server for a DB2 product (for example, Database Performance for DB2), and a Installation System server for an IMS product (for example, RECOVERY MANAGER for IMS), you can merge the two Installation System servers into a single Installation System server and a single started task procedure.

The single Installation System server will then work with both products.

To merge multiple products into one Installation System server

1. Locate the #UIM member that the Installation System created in the Installation System sample library.
2. Copy the #UIM member to your system procedure library and give the new member the name that you selected for the startup member during installation.
3. Ensure that the new Installation System load library (HLQ.XXLINK) is first in the STEPLIB concatenation.
4. Add the older versions of the following files in concatenation order after the newer versions:
   - Application load library
   - Configuration file (see Example of the Installation System Concatenated Configuration File (see page 241) for an example)
   - Content file (see Example of Installation System Content Concatenated Files (see page 241) for an example)
4. **Note**

The content files and the configuration files must be ordered from newest products and files to the oldest products and files.

If you have installed the BMC System Performance for DB2 solution version 3.2.00 or earlier, you must specify the CONFIG library for that product as the last configuration file in the list.

**Example of the Installation System Concatenated Configuration File**

<table>
<thead>
<tr>
<th>DD</th>
<th>DISP</th>
<th>DSN</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTPARM</td>
<td></td>
<td>DSN=HLQ.XXCNFG</td>
<td>new UIM configuration library</td>
</tr>
<tr>
<td></td>
<td>DISP</td>
<td>DSN=HLQ.IMCNFG</td>
<td>from merged IMS install</td>
</tr>
<tr>
<td></td>
<td>DISP</td>
<td>DSN=HLQ.productCodeCNFG</td>
<td>from nonmerged IMS install</td>
</tr>
<tr>
<td></td>
<td>DISP</td>
<td>DSN=HLQ.CONFIG</td>
<td>from new DFD install</td>
</tr>
</tbody>
</table>

**Example of Installation System Content Concatenated Files**

<table>
<thead>
<tr>
<th>DD</th>
<th>DISP</th>
<th>DSN</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTPCONT</td>
<td></td>
<td>DSN=HLQ.XXCONT</td>
<td>new UIM configuration library</td>
</tr>
<tr>
<td></td>
<td>DISP</td>
<td>DSN=HLQ.IMCONT</td>
<td>from merged IMS install</td>
</tr>
<tr>
<td></td>
<td>DISP</td>
<td>DSN=HLQ.productCodeCONT</td>
<td>from nonmerged IMS install</td>
</tr>
<tr>
<td></td>
<td>DISP</td>
<td>DSN=HLQ.CONT</td>
<td>from new DFD install</td>
</tr>
</tbody>
</table>

**Note**

Use only the files that you currently have in the concatenation.

The following figure shows an example of a consolidated started task procedure for the Installation System server. The product application load library, content file, and configuration file are the newer versions.

**Example—Consolidated #UIM member**

```plaintext
//configMember PROC M=configMember,           PGM=UIMMAIN, REGION=0K, ENV= 
```
// TIME=1440,ACCT=(5210),
// PARM=('C &M &ENV -L =B =CNFTRACE =S -U =VERSION')

/* COMMON COMMAND-LINE PARAMETERS:
   -C MMMMMM  CONFIGURATION FILE MEMBERNAME
   -P 9999  TCP LISTENER PORT NUMBER
   -L       LOG MESSAGES AND TRACE VIA SUBTASK
   -SOUT=    SPECIFY THE SYSOUT CLASS FOR DYNAMICALLY ALLOCATED
             LOG FILES( IE. -SOUT=X )
   =B        PRINT FUNCTION TRACEBACK WITH LIBRARY WARNINGS
   =CNFTRACE PRINT DIAGNOSTICS DUE TO TCP/IP CONFIGURATION FAILURES
   =S        PRINT STORAGE ANALYSIS REPORT AT TERMINATION
   =U        PRINT STORAGE USAGE REPORT AT TERMINATION
   =VERSION  PRINT RUNTIME LIBRARY RELEASE INFORMATION TO SYTERM

STEPLIB DD DISP=SHR,DSN=HLQ.XXLINK <--from new UIM/DHS install
       DD DISP=SHR,DSN=HLQ.IMLOAD <--from merged IMS install
       DD DISP=SHR,DSN=HLQ.productCodeLOAD <--from nonmerged IMS
       DD DISP=SHR,DSN=DB2HLQ.DSNEXIT <--if DB2 products are
       installed
       DD DISP=SHR,DSN=DB2HLQ.DSNLOAD <--if DB2 products are
       installed

SAS/C DD'S
SYSTERM DD SYSOUT=*  //SYSPRINT DD SYSOUT=*  //STGRPT DD SYSOUT=*  //APPLICATION SERVER DD'S
5. Restart the Installation System server address space.

Sharing UIM server with multiple IMS products

If you have installed multiple IMS products you can use one UIM server for all the products.

If you are installing both IMS and DB2 products on the same UIM server, see the instructions in Merging multiple products into a single UIM server (see page 240).

For IMS products to work together and share a UIM server, ensure that the CPC started task name has been created with a suffix of ADV. For example, CPCxADV.

⚠️ Note

If you need to change the started task name, you must update the CPCxCMDS to issue CPC START ADV instead of CPC START IPT that was originally created during IPT customization.
Creating a new UIM server

When the UIM server was installed, the sample startup procedure was copied, customized, and saved in your sample library. You may want to create additional UIM servers.

Creating a new UIM server comprises several tasks. Each high-level task includes several steps. The tasks are:

1. Creating a startup configuration member (see page 244)
2. Creating a started task procedure (see page 245)
3. Allocating the HFS data set (see page 247)
4. Initializing the HFS data set (see page 248)
5. Enabling and disabling password caching (see page 257)

Creating a startup configuration member

Since the UIM server requires a startup configuration member, you must create a member for the new UIM server.

To create a startup configuration member

1. Locate the #NORMAL member in the UIM sample library.
2. Create a startup configuration member by copying the #NORMAL member from your product sample library into your configuration file and giving it a new name.
   The following figure shows the startup configuration member. The hlq shown in this member is the high-level qualifier that you specified during installation.

   **Startup configuration member**

   ```xml
   <bmchttp>
   <bmc_parm id="PORT" value="9999" />  
   <bmc_parm id="AUTH_TIMEOUT_SECS" value="1800" />  
   <bmc_parm id="AFF_TIMEOUT_SECS" value="1800" />  
   <bmc_parm id="HFS_DATASET" value="hlq.HFS" />  
   <bmc_parm id="ALLOW_NETCMD" value="YES" />  
   </bmchttp>
   ``

3. Edit the new startup configuration member by changing the variables that are listed in the following table.

   **Startup configuration member variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted value</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;BMC_PARM ID=' PORT' VALUE=' 9999' /&gt;</td>
<td>Port value for the UIM server</td>
<td>Unique numeric value that is between 1 and 65535</td>
<td>Changing the port number (see page 250)</td>
</tr>
</tbody>
</table>
### Variable Definition

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted value</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;BMC_PARM ID=&quot;AUTH_TIMEOUT_SECS&quot; VALUE=&quot;1800&quot;/&gt;</td>
<td>Security authorization timeout for the console</td>
<td>Numeric value in seconds</td>
<td>Changing the security authorization timeout feature permanently (see page 251)</td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;AFF_TIMEOUT_SECS&quot; VALUE=&quot;1800&quot;/&gt;</td>
<td>Idle timeout period for affinity tasks</td>
<td>Unique numeric value in seconds</td>
<td>Changing the idle timeout for affinity tasks (see page 252)</td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;HFS_DATASET&quot; VALUE=&quot;hlq.HFS&quot;/&gt;</td>
<td>HFS data set name</td>
<td>PDSE data set name for storing the HFS data</td>
<td>Changing the HFS server-side storage data set name (see page 252)</td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;ALLOW_NETCMD&quot; VALUE=&quot;YES&quot;/&gt;</td>
<td>Enable or disable network browser command interface</td>
<td>YES (default), NO or AUTHORIZE</td>
<td>Enabling or disabling the network browser command interface (see page 253)</td>
</tr>
</tbody>
</table>

---

### Creating a started task procedure

After creating the startup configuration member, you must create a started task procedure for that startup member.

**To create a started task procedure**

1. Locate the #UIM member in the UIM sample library.
2. Create a new #UIM member by copying the #UIMx member to your system procedure library and giving the new member the name that you selected for the startup member (see Creating a startup configuration member (see page 244)).

The following figure shows the #UIM member.

#### #UIM member

```plaintext
//uimx PROC M=uimx,           <----- NAME OF CONFIGURATION MEMBER
// ENV=
//*--------------------------------------------------------------
//uimx EXEC PGM=UIMMAIN, +
//   ACCT=(acct),       <--- SPECIFY ACCOUNTING INFO +
//   REGION=0K,         <--- SPECIFY REGION SIZE +
//   TIME=1440,         +
// PARM=(' -C &M &ENV -L =B =CNFTRACE =VERSION')
//*
//* COMMON COMMAND-LINE PARAMETERS:
//*
//* -C MMMMMM  CONFIGURATION FILE MEMBERNAME
//* -P 9999  TCP LISTENER PORT NUMBER
//* -L  LOG MESSAGES AND TRACE VIA SUBTASK
//*
```
2. /*- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
*/ ENVIRONMENT VARIABLES TO Control EXECUTION:
/*
*/ -SOUT= SPECIFY THE SYSOUT CLASS FOR DYNAMICALLY ALLOCATED
*/ LOG FILES( IE. -SOUT=X )
/*
*/- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
*/ SAS/C RUNTIME LIBRARY PARAMETERS:
/*
*/ -CNFTRACE PRINT DIAGNOSTICS DUE TO TCP/IP CONFIGURATION FAILURES
/*
*/ -VERSION PRINT RUNTIME LIBRARY RELEASE INFORMATION TO SYSTERM
/*
*/- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
*/STEPLIB DD DISP=SHR,DSN=bmc.uim.load
// DD DISP=SHR,DSN=bmc.pch.load
/*
*/ SAS/C DD'S
/*
*/SYSTERM DD SYSOUT=* 
*/SISPRINT DD SYSOUT=* 
*/STGRPT DD SYSOUT=* 
/*
*/APPLICATION SERVER DD'S
/*
*/MSGLOG DD SYSOUT=* 
*/TRCLOG DD SYSOUT=* 
*/HTPCONT DD DISP=SHR,DSN=bmc.uim.content
*/HTPPARM DD DISP=SHR,DSN=bmc.uim.config
/*
*/STDERR03 DD DUMMY MSG LOGGER
*/STDERR04 DD DUMMY TRACE LOGGER
*/STDERR05 DD DUMMY RR LOGGER
/*
*/STANDARD JOB DD'S
/*
*/SYSUDUMP DD SYSOUT=* 

3. Edit the new #UIMx member by changing the variables that are listed in the following table.

**#UIMx member variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted value</th>
</tr>
</thead>
<tbody>
<tr>
<td>uimx</td>
<td>Name of the started task procedure and the startup configuration member</td>
<td>Name that you gave to the #UIMx member when you copied it to your system procedure library (Step 2 (see page 245))</td>
</tr>
<tr>
<td>bmc.uim.load</td>
<td>Library that contains the UIM server and product execution code</td>
<td>Valid data set name</td>
</tr>
<tr>
<td>bmc.pch.load</td>
<td>Library that contains your product code</td>
<td>Valid data set name</td>
</tr>
<tr>
<td></td>
<td>Library that contains code and files get downloaded to the console during installation of the console</td>
<td>Valid data set name</td>
</tr>
</tbody>
</table>
### Setting up the HFS data set

After creating the startup configuration member and the started task procedure, you can allocate and initialize the HFS data set.

This server-side storage data set stores user preferences and dynamic configuration information on the UIM server. During installation, the hlq.HFS member in the SAMP library was created and customized with your site specific information. You can submit the customized data set, or you can customize a copy of the data set member in the sample library.

You can share the HFS data set between all UIM servers within a Sysplex or all of the LPARs that share the DASD complex. You can also create a unique HFS data set for each UIM. One of the advantages of sharing the HFS data set is to gain sharing of console client Enterprise Connection list.

### Allocating the HFS data set

After creating the startup configuration member and the started task procedure, you can allocate the HFS data set.

During installation, the hlq.HFS member in the SAMP library was created and customized with your site specific information. You can submit the customized data set, or you can customize a copy of the data set member in the sample library.

### To customize a copy of the data set member

1. Locate the #DEFHFS member in the UIM sample library.
   The following figure shows the #DEFHFS member. `hlq` in this member is the high-level qualifier that you specified during installation.

   **Default #DEFHFS member**

   ```
   //ALLPDSE EXEC PGM=IEFBR14
   //HFSPOSE DD DISP=(NEW,CATLG),UNIT=SYSDA,SPACE=(CYL,(1,1)),
   //   DCB=(DSORG=PO,RECFM=VB,LRECL=4096),
   //   DSNTYPE=LIBRARY,
   //   DSN=<hlq>.HFS
   ```

2. Edit the #DEFHFS member by changing the variables that are listed in the following table.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bmc.uim.content</td>
<td>Library that contains common UIM server, console code, and product execution parameters are used during initialization of the UIM server</td>
<td>Valid data set name</td>
</tr>
</tbody>
</table>
#DEFHFS member variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIT</td>
<td>Device for placing data sets</td>
<td>See your site standards</td>
</tr>
<tr>
<td>DSN</td>
<td>High-level qualifier</td>
<td>See your site standards</td>
</tr>
</tbody>
</table>

3. Save the edited #DEFHFS member with a new name.
4. Submit the DEFHFSJC member JCL.

Initializing the HFS data set

Before you can share connections in a sysplex, you must initialize the HFS data set that you allocated. During installation, the HFSLOAD data set is created and customized with your site-specific information.

To submit a copy of the customized data set member

1. Locate #LOADHFS in the UIM sample library data set.

   The following figure shows the default #LOADHFS member.

   **Default #LOADHFS member**

   ```
   //*--------------------------------------------------------------
   //*     Load the BMC HFS PDSE with SAMP library members.
   //*     Optionally convert previous BMC HFS HostList.xml if found.
   //*--------------------------------------------------------------
   //LOADHFS EXEC PGM=UIMHFSL,REGION=0K,
   //  PARM='=version $UIMHFSL $UIMHFST'
   //*-  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
   // UIMHFSL parameters:
   ///
   ///   memname    Samplib control cards member, default is $HFSLOAD.
   ///
   ///      - $HFSLOAD is a Load of default properties files
   ///   -t     Activate tracing to SYSPRINT
   ///
   // SAS/C Runtime Library parameters:
   ///
   ///   -version  Print Runtime Library release information to SYSTERM
   ///
   // STEPLIB  DD  DISP=SHR,DSN=?????????.LOAD
   ///
   ///   SAS/C DD'S
   /// SYSTEM DD SYSOUT=*  
   /// SYSPRINT DD SYSOUT=*  
   /// STGRPT DD SYSOUT=*  
   ///
   /// STANDARD JOB DD'S
   /// SYSUDUMP DD SYSOUT=* 
   ```
2. Edit the #LOADHFS member, and change ??????????? to the high-level qualifier according to your site standards.
3. Save the edited member as HFSLOAD.

```
//*
//HFSPDSE DD DISP=SHR,DSN=?????????.HFS
//SAMP   DD DISP=SHR,DSN=?????????.SAMP
//CONT   DD DISP=SHR,DSN=?????????.CONTENT
//*
```

4. Submit the HFSLOAD member JCL.

## Customizing the UIM server

The UIM server is configured during installation.

However, you can view or alter the original configuration of the UIM server permanently by changing the values for variables in the startup and trace members of the configuration file. For information about changing the configuration setting temporarily, see the instructions for operating the UIM server in your product documentation.

You can change the following UIM server configuration options:

- Port number
- Authorization security timeout
- Affinity timeout
- Server-side storage data set (HFS data set)
- Tracing
- Enable/disable network browser command interface

Each UIM server requires a configuration member, called the startup member, that describes the unique characteristics of each server. This member is specified as a parameter in the UIM server configuration file.

The sample library (hlq.SAMP) contains a template for the startup member named #NORMAL. The installation process customizes the #NORMAL member, gives it the same name as the started task procedure, and copies it to the hlq.CONFIG data set.

The following figure shows the #NORMAL member template.
#NORMAL member template

```xml
<bmchttp>
    <bmc_parm id="PORT" value="9999" />
    <bmc_parm id="AUTH_TIMEOUT_SECS" value="1800" />
    <bmc_parm id="AFF_TIMEOUT_SECS" value="1800" />
    <bmc_parm id="HFS_DATASET" value="hlq.HFS" />
    <bmc_parm id="ALLOW_NETCMD" value="YES" />
</bmchttp>
```

The editable variables in the #NORMAL member are defined in the following table.

#NORMAL member variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted Value</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;BMC_PARM ID='PORT' VALUE='9999'&gt;</code></td>
<td>Port value for the UIM server</td>
<td>Unique numeric value</td>
<td>Changing the port number (see page 250)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that is between 1 and 65535</td>
<td></td>
</tr>
<tr>
<td><code>&lt;BMC_PARM ID='AUTH_TIMEOUT_SECS' VALUE='1800'</code></td>
<td>Timeout for security authorization</td>
<td>Numeric value in</td>
<td>Changing the security authorization timeout feature permanently (see page 251)</td>
</tr>
<tr>
<td><code>/&gt;</code></td>
<td></td>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td><code>&lt;BMC_PARM ID='AFF_TIMEOUT_SECS' VALUE='1800'</code></td>
<td>Idle timeout period for affinity tasks</td>
<td>Unique numeric value</td>
<td>Changing the idle timeout for affinity tasks (see page 252)</td>
</tr>
<tr>
<td><code>/&gt;</code></td>
<td></td>
<td>in seconds</td>
<td></td>
</tr>
<tr>
<td><code>&lt;BMC_PARM ID='HFS_DATASET' VALUE='hlq.HFS'</code></td>
<td>HFS data set name</td>
<td>PDSE data set name</td>
<td>Changing the HFS server-side storage data set name (see page 252)</td>
</tr>
<tr>
<td><code>/&gt;</code></td>
<td></td>
<td>for storing HFS data</td>
<td></td>
</tr>
<tr>
<td><code>&lt;BMC_PARM ID='ALLOW_NETCMD' VALUE='YES'</code></td>
<td>Enable or disable network browser command interface</td>
<td>YES (default), NO, or AUTHORIZE</td>
<td>Enabling or disabling the network browser command interface (see page 253)</td>
</tr>
</tbody>
</table>

Changing the port number

The port number for the UIM server is the address of a TCP/IP application, in this case the UIM server, on a z/OS image.

The UIM server has one port number that consoles use to contact the UIM server. You can change the port number globally for all consoles that communicate with the UIM server.

To change the port number

1. Edit your startup configuration member.

**Note**
The startup member name is typically the same as the started task procedure name for the UIM server.

2. In your startup configuration member, find the PORT variable.
   The default port number is 9999.
   The PORT variable is displayed as follows:
   
   `<bmc_parm id="PORT" value="9999" />`

3. Change the value of BMC_PARM ID='PORT' from 9999 to a unique numeric value between 1 and 65535.

   Warning
   Check with your TCP/IP administrator to ensure that you are entering a unique port number. If you do not enter a unique port number, program errors may occur.

Changing the security authorization timeout feature permanently

The console is equipped with a timeout security feature.

This feature controls the amount of time that all consoles which communicate with the UIM server can remain inactive before security authorization expires. This value is set during installation. You can change the timeout feature permanently for all consoles that communicate with the UIM server.

To change the security authorization timeout feature temporarily, see the instructions for operating the UIM server in your product documentation.

To change the timeout feature permanently

1. Edit your startup configuration member.

   Note
   The startup member name is typically the same as the started task procedure name for the UIM server.

2. From your startup configuration member, find the AUTH_TIMEOUT_SECS variable.
The default number of seconds is 1800.
The AUTH_TIMEOUT_SECS variable is displayed as follows:

```xml
<bmc_parm id="AUTH_TIMEOUT_SECS" value="1800" />
```

3. Change the value of BMC_PARM ID='AUTH_TIMEOUT_SECS' from 1800 to any numeric value in seconds.

**Changing the idle timeout for affinity tasks**

Affinity timeout is the amount of time that the task is held between requests for the affinity.

When the task is inactive for the defined period, the affinity is no longer valid and the task is available for other work.

**To change the idle timeout for affinity tasks**

1. Edit your startup configuration member.

   ![](Note)

   The startup member name is typically the same as the started task procedure name for the UIM server.

2. From your startup configuration member, find the AFF_TIMEOUT_SECS variable.
The default number of seconds is 1800.
The AFF_TIMEOUT_SECS variable is displayed as follows:

```xml
<bmc_parm id="AFF_TIMEOUT_SECS" value="1800" />
```

3. Change the value of BMC_PARM ID='AFF_TIMEOUT_SECS' from 1800 to any numeric value in seconds.

**Changing the HFS server-side storage data set name**

The HFS server-side storage data set stores user preferences and dynamic configuration information on the UIM server.

**To change the HFS data set name**

1. Edit your startup configuration member.
Note

The startup member name is typically the same as the started task procedure name for the UIM server.

2. From your startup configuration member, find the HFS_DATASET variable.
   The HFS_DATASET variable contains the data set name to use for the UIM server server-side storage data set.
   The HFS_DATASET variable is displayed as follows:

```
<bmc_parm id="HFS_DATASET" value="<hlq>.HFS" />
```

3. Change the value of the high-level qualifier for HFS_DATASET from hlq to a value that meets your site standards.

Enabling or disabling the network browser command interface

The network browser command interface, also known as the BMC UIM server Commands web page, displays UIM server information and allows an administrator to make dynamic modifications to UIM server settings.

You can enable or disable the network command interface. You can also provide an active authentication with the browse session. Once the variable ALLOW_NETCMD is set to AUTH, the user must log in using the following command in the web browser:

```
http://uimServerHostName:uimPortNumber/UIMLogon
```

If the logon is successful, the user can display the BMC UIM server Commands web page (http://uimServerHostName:uimPortNumber/httpcmd.html). For more information about the BMC UIM server Commands web page, see the instructions for operating the UIM server in your product documentation.

To enable or disable the network browser command interface

1. Edit your startup configuration member.
2. From your startup configuration member, find the ALLOW_NETCMD variable.
   By default, the network browser commands are processed by the UIM server, but they may be disabled by setting the ALLOW_NETCMD value to NO.
   The ALLOW_NETCMD variable is displayed as follows:

```
<bmc_parm id="ALLOW_NETCMD" value="YES" />
```

3. Change the ALLOW_NETCMD value to one of the following values:
Enabling or disabling the overall tracing option permanently

This product was shipped with the recommended tracing options preset.

Each UIM server requires a trace configuration member, called the TRACE member, that defines the tracing for each server. To change the overall tracing option temporarily, see 'Enabling or disabling the overall tracing option temporarily' in the Troubleshooting section.

The sample library contains a trace configuration member named TRACE. During installation, the TRACE member is copied to the hlq.CONFIG file.

TRACE member

```xml
<bmchttp>
  <rlog value="OFF" />
  <trace value="ON">
    <bmc_parm id="TRACE_ACTION" value="TRACEACTION_WARNING" />
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_INFO' /-->
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_ENTRYEXIT' /-->
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_CONTROL' /-->
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_MEMORY' /-->
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_SOCKET' /-->
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_THREAD' /-->
    <!-- BMC_PARM ID='TRACE_ACTION' VALUE='TRACEACTION_WAIT' /-->
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_SERVER" />
    <!-- BMC_PARM ID='TRACE_COMPONENT' VALUE='TRACECOMPONENT_SERVER_WL' /-->
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_CLIENT" />
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_REQUEST" />
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_EXTENSION" />
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_TASKMGR" />
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_TASKWR" />
    <!-- BMC_PARM ID='TRACE_COMPONENT' VALUE='TRACECOMPONENT_LOGTASK' /-->
    <bmc_parm id="TRACE_COMPONENT" value="TRACECOMPONENT_EXTERNAL" />
  </trace>
</bmchttp>
```
Note

BMC recommends that you change the trace configuration member only with direction from BMC Customer Support.

To change the overall tracing option permanently

1. Edit your trace configuration member.
2. From your trace configuration member (see page 254), find the TRACE VALUE variable.
3. To enable or disable the overall tracing option, perform one of the following tasks:
   - To enable the overall tracing option, type ON inside the quotation marks.
     For example:

     `<trace value="ON">`

   - To disable the overall tracing option, type OFF inside the quotation marks.
     For example:

     `<trace value="OFF">`

4. Verify that the TRACE VALUE has been enabled or disabled.

Enabling or disabling specific tracing options permanently

The product was shipped with the recommended specific tracing options preset.

This section describes how to change specific tracing options permanently.

Note

BMC recommends that you change the trace configuration member only with direction from BMC Customer Support.

To verify that the overall tracing option is enabled

1. Edit your trace configuration member.
   The figure in Enabling or disabling the overall tracing option permanently (see page 254) shows the trace configuration member.
2. Ensure that the overall trace option is enabled.
   If the overall trace option is enabled, the variable is displayed as follows:
3. If the overall trace option is not enabled, edit the variable as required to enable it.

To enable specific tracing options

1. From the list of specific tracing options, find the option that you want to enable.

   Example

   ```xml
   <!-- BMC_PARM    ID='TRACE_ACTION'
   VALUE='TRACEACTION_INFO' /-->
   ```

2. Remove the exclamation point, hyphens, and space (!-- ) that are displayed between the opening bracket (<) and text (BMC_PARM).
3. Remove the hyphens (-- ) that are displayed between the forward slash (/) and the closing bracket (>).
   The specific tracing option is enabled and is displayed as follows:

   ```xml
   <bmc_parm id="TRACE_ACTION" value="TRACEACTION_INFO" />  
   ```

To disable specific tracing options

1. From the list of specific tracing options, locate the option that you want to disable.

   Example

   ```xml
   <bmc_parm id="TRACE_ACTION" value="TRACEACTION_INFO" />  
   ```

2. Type an exclamation point, two hyphens, and a space (!-- ) between the opening bracket (<) and text (BMC_PARM).
3. Type two hyphens (-- ) between the forward slash (/) and the closing bracket (>).
   The specific tracing option is disabled and is displayed as follows:
Enabling and disabling password caching

By default, when you log on to the console or when you create connections, the console caches the password.

To enable or disable password caching

1. Locate member #UPDADM in the SAMP library.
   The following figure shows the default member #UPDADM.

   Default member #UPDADM

   ```
   //***************************************************************
   //** Load the BMC HFS PDSE with SAMP library member to update the **
   //** Password Caching setting.                                **
   //***************************************************************
   //UPDADM  EXEC PGM=UIMHFSL,REGION=0K,                     
   //  PARM='=b =version $UPDADM'                           
   //  memname   Samplib control cards member, default is $HFSLOAD. 
   //  - $UPDADM is an update of Password cache member only 
   //  -t        Activate tracing to SYSPRINT                 
   //***************************************************************
   //STEPLIB  DD  DISP=SHR,DSN=?????????.LOAD                  
   //***************************************************************
   //SAS/C DD'S                                               
   //SYSTERM  DD  SYSOUT=*                        
   //SYSPRINT DD  SYSOUT=*                   
   //STGRPT  DD  SYSOUT=*                       
   //***************************************************************
   //STANDARD JOB DD'S                               
   //SYSUDUMP DD  SYSOUT=*                          
   //***************************************************************
   //HFSPDSE  DD  DISP=SHR,DSN=?????????.HFS         
   //SAMP     DD  DISP=SHR,DSN=?????????.SAMP         
   ```

2. Edit member #UPDADM, and change ?????????????? to the high-level qualifier according to your site standards.
3. Save the edited member as UPDADMIN.
4. Locate member $ADMIN in the SAMP library.
   The following figure shows the default member $ADMIN.

   Default member $ADMIN
AllowPasswordCaching=true

5. Perform one of the following actions:
   - To disable password caching, set AllowPasswordCaching to false.
   - To enable password caching, set AllowPasswordCaching to true.
6. Save $ADMIN.
7. Submit the member UPDADMIN JCL.

Operating subsystems and product servers

This section discusses the subsystems and product server that are associated with BMC System Administration for IMS. The following topics are covered in this section:

- Overview of customizing BMC System Administration for IMS (see page 258)
- Operating the BMCP subsystem (see page 259)
- Operating the BCSS/CPC subsystem (see page 260)
- Operating the IPT server (see page 263)

Overview of customizing BMC System Administration for IMS

The following subsystems and product server are associated with BMC System Administration for IMS:

- BMCP subsystem
- BCSS/CPC subsystem
- IPT server
- IPT repositories

⚠️ Note

- The STEPLIB libraries must be APF-authorized for the BMCP subsystem.
- The STEPLIB libraries must be APF-authorized for the BCSS/CPC subsystem unless they are in the LINKLIST. Libraries in the LINKLIST are already APF-authorized.
Operating the BMCP subsystem

The BMCP subsystem establishes supervisory services for many BMC products.

Because BMC products share a single BMCP subsystem, you can have only one copy of it on an MVS.

Always use the latest version of the BMCP subsystem. Use the BCSCHECK program to determine whether an earlier version of the BMCP subsystem is installed on your system. For details about the BCSCHECK program, see the BMC Software Subsystems User Guide.

BMC recommends that the BMCP subsystem always remain active. However, you must terminate a subsystem to install maintenance modules for that subsystem.

For detailed information about the BMCP subsystem, see the BMC Software Subsystems User Guide.

Started task procedure name for BMCP

The default started task procedure name for the BMCP subsystem is BMCP. You must use the default procedure name for BMCP.

The Installation System customized the BMCP started task procedure name for you. It is stored in the data set that you specified in the UIM Customized Parm Library field on the UIM server Middleware Options panel. For information about the panel, see the Installation System Reference Manual.

BMCP subsystem commands

Use one of the following methods to execute BMCP subsystem commands:

- Place the commands in a COMMNDxx member of SYS1.PARMLIB so that they are issued automatically during an IPL.
- Issue the commands from the operator console.

The following table lists BMCP subsystem commands. In the sample command, the started task procedure name used for the BMCP subsystem is BMCP. If you experience problems, review the system log to ensure that your commands completed successfully.

<table>
<thead>
<tr>
<th>Task</th>
<th>Sample command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the BMCP subsystem</td>
<td>START BMCP</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
</tbody>
</table>
### Operating the BCSS/CPC subsystem

The BCSS/CPC subsystem manages APF-authorized functions and performs processing for intercepted MVS requests.

Only one public BCSS is allowed on an MVS; however, you can have multiple private BCSSs. BMCP allows the public BCSS first access to an intercepted request and ensures that the appropriate BCSS receives control when required.

BMC System Administration for IMS uses the BCSS subsystem in conjunction with CPC technology. If CPC is installed with the BCSS subsystem, the solution can share a BCSS subsystem with other BMC products.

Always use the latest version of the BCSS subsystem. Use the BCSCHECK program to determine whether an earlier version of BCSS is installed on your system. For details about the BCSCHECK program, see the *BMC Software Subsystem User Guide*.

BMC recommends that the BCSS/CPC subsystem always remain active. However, you must terminate a subsystem to install maintenance modules for that subsystem.

For detailed information about the BCSS subsystem, see the *BMC Software Subsystem User Guide*.

### Started task procedure name for BCSS/CPC

The default started task procedure name for the BCSS/CPC subsystem is CPC x. The suggested name for the subsystem when used with BMC System Administration for IMS is IPTA.

**Note**

The variable x must be the same value for CPC x, CPCxIPT, and UIMx (procedure name for the UIM server).
The Installation System customized the BCSS/CPC started task procedure name for you. It is stored in the data set that you specified in the UIM Customized Parm Library field on the UIM server Middleware Options panel. For more information about the panel, see the Installation System Reference Manual.

BCSS/CPC installation

During the installation process, you entered CPC information that was used to tailor JCL to generate and start the IPT server and to allocate the IPT repository.

For more information, see the installation guide.

⚠️ Note

For information about a possible CPC initialization failure, see the Installation System Reference Manual.

CPC components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>The console is the graphical user interface (GUI). The console runs on a client workstation under the Microsoft Windows operating system and communicates with the UIM server through TCP/IP technology.</td>
</tr>
<tr>
<td>UIM server</td>
<td>The UIM server resides on the mainframe and handles communication between the console and BMC console-enabled mainframe products and features.</td>
</tr>
<tr>
<td>IPT server</td>
<td>The IPT server is the BMC System Administration for IMS product server. BMC System Administration for IMS uses the IPT server to communicate with the UIM server, IPT repositories, IMS subsystems, and IMS databases.</td>
</tr>
<tr>
<td>IPT repositories</td>
<td>The IPT repositories are VSAM data sets. The IPT repositories store information used by BMC System Administration for IMS for processing information.</td>
</tr>
<tr>
<td>BCSS/CPC subsystem</td>
<td>The BCSS subsystem manages APF-authorized functions and performs processing for intercepted MVS requests. If CPC was installed with BCSS, console-enabled BMC products for IMS can share a BCSS with other BMC products. Always use the latest version of the BCSS subsystem. To determine whether an earlier version of BCSS is installed on your system, use the BCSCHECK program. For more information about the BCSCHECK program, see the BMC Software Subsystems User Guide. BMC recommends that the BCSS/CPC subsystem always remain active. However, you must terminate a subsystem to install maintenance modules for that subsystem.</td>
</tr>
<tr>
<td>IMS subsystems</td>
<td>Console-enabled BMC products for IMS retrieve information about active IMS subsystems and the databases that are defined to the IMS subsystems. The information is used by the products during processing.</td>
</tr>
</tbody>
</table>
### JCL requirements

The installation procedure customized the IPT server JCL for you.

You must modify `your.system.proclib` to reflect the system procedure library name where all members reside. The installation procedure does not automatically copy the customized procedures to your system procedure library.

The installation procedure performs the following actions:

- *(if load library is in the LINKLIST)* Removes the STEPLIB
- Modifies `hlq.CPCLIB` (if you chose non-merged libraries for your installation) or `hlq.IMLIB` (if you chose merged libraries for your installation) to your product load library

For information about installation libraries, see the *Installation System Reference Manual*.

### BCSS/CPC subsystem commands

The BCSS/CPC subsystem must be active to start BMC System Administration for IMS.

Use one of the following methods to execute BCSS/CPC subsystem commands:

- Place the commands in a `COMMAND.xx` member of `SYS1.PARMLIB` so they are issued automatically during an IPL.
- Place the commands in a BCSS/CPC commands data set so they are issued at BCSS/CPC startup. Member `CPCxCMDS` in `CPCSAMP` (if you chose non-merged libraries for your installation) or `IMSAMP` (if you chose merged libraries for your installation) contains sample BCSS/CPC commands. For information about non-merged and merged installation libraries, see the installation guide.

  **Tip**

  If you use the `CPCxCMDS` data set member, BCSS/CPC starts the IPT server automatically.

- Issue the commands from the operator console.

The following table describes BCSS/CPC subsystem commands. In the sample command, the started task procedure name that is used for the BCSS/CPC subsystem is `IPTA`. If you experience problems, review the system log to ensure that your commands completed successfully.

### BCSS/CPC subsystem commands
Operating the IPT server

The IPT server provides the technology for communication among clients and the BMC System Administration for IMS solution.

If a cpdxCMDS data set member contains the default CPC START IPT command, the IPT server automatically starts when you start the BCSS/CPC subsystem. If the BCSS/CPC subsystem does not automatically start the IPT server, you must start the IPT server manually.

Although you can have multiple server address spaces on one MVS, BMC recommends that you have as few address spaces as are required to avoid connectivity issues.

Started task procedure name for IPT

The default started task procedure name for the IPT server is cpdxIPT, where cpdx is the BCSSID. BMC recommends that you use the default procedure name for the IPT server.

The installation procedures customized the IPT server started task procedure name for you. The started task procedure name for the IPT server matches the name that you selected for the BCSS/CPC subsystem. The started task procedure name for the IPT server is stored in CPCSAMP (if you chose non-merged libraries for your installation) or IMSAMP (if you chose merged libraries for your installation). For information about non-merged and merged installation libraries, see the installation guide.

Execute the started tasks for the IPT server from a JES2 procedure library that is shared by all MVS images in your environment.

CPCINI and CPCTRRC DD statements must point to the following members:

- cpdxINI
- cpdxTRC
The CPCINI DD statement must be specified in the IPT server started task procedure. The default cpcxINI member in CPCSAMP (if you chose non-merged libraries for your installation) or IMSAMP (if you chose merged libraries for your installation) contains sufficient keywords for normal operations. For information about non-merged and merged installation libraries, see the installation guide.

**Security**

The user ID that is assigned to the IPT server address space must have the following authority:

- **UPDATE/ALTER** authority to create and update IPT repository data sets and to issue operator commands
  - The prefix for the VSAM data sets that make up the IPT repository data sets is specified in the CPCINI file REP control statement.
- **READ** authority to IMS system data sets
- **READ** authority to access the databases that the BMC System Administration *for IMS* solution accesses

Authority is defined in RACF configuration.

**Sysplex implementation**

In a sysplex environment, it is preferable that IPT server address spaces communicate with each other so that repository data can be shared.

TSO users can access all repository data, regardless of the MVS system to which they log on. Data is maintained in a single repository, regardless of the MVS system on which the utility executes.

There can be only one master IPT server. All other IPT servers are considered slaves. The master IPT server initiates all required functions for the product. When creating the cpcxINI file for a sysplex, you must decide which of the following ways that you want the IPT servers to communicate.

- 

  *(recommended)* Designate a master IPT server that always initiates all of the functions that are required for the BMC System Administration *for IMS* solution to run. If you use this method, BMC recommends that you always start the master IPT server first.
  - If the designated master IPT server starts successfully but later becomes unavailable, another CPC server (slave) becomes the master. When the designated master becomes available again, control is passed back to the designated master and the other CPC server returns to slave status.
  - If the designated master IPT server does not start, the other CPC servers wait for one hour before issuing an ABEND.
During the installation process, a `cpcxINI` file was created in CPCSAMP (if you chose non-merged libraries for your installation) or IMSAMP (if you chose merged libraries for your installation). It contains the XSYS command that designates the master IPT server. For information about non-merged and merged installation libraries, see the installation guide. For information about the XSYS command, see the Master keyword in CPCINI keywords (see page 267).

- If a master IPT server was not designated, the first active CPC becomes the master and initiates all required functions. If the master fails, another CPC becomes the master and takes over all required functions. If the first CPC IPT server becomes active again, it returns as a slave.

## IPT server commands

The following table lists the IPT server commands that you can use to start and stop the IPT server.

If you experience problems, review the system log to ensure that your commands completed successfully.

### IPT server commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually start the IPT server</td>
<td><code>cpcx CPC START IPT</code></td>
</tr>
<tr>
<td>Manually stop the IPT server</td>
<td><code>cpcx CPC STOP IPT</code></td>
</tr>
</tbody>
</table>

The following table lists the IPT server operator console command tasks.

### IPT server operator console commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write all trace information to the specified SYSOUT class when the CPCTRACE data set is allocated</td>
<td><code>cpcx CPC IPT TRACE SYSOUT (*)</code></td>
<td>TRACE SYSOUT (see page 266)</td>
</tr>
<tr>
<td>Write all trace information to the CPCTRACE data set</td>
<td><code>cpcx CPC IPT TRACE SPILL(n)</code></td>
<td>TRACE SPILL (see page 266)</td>
</tr>
<tr>
<td>Write all log information to the specified SYSOUT class when the CPCLOG data set is allocated</td>
<td><code>cpcx CPC IPT LOG SYSOUT (*)</code></td>
<td>LOG SYSOUT (see page 267)</td>
</tr>
<tr>
<td>Write all log information to the CPCLOG data set</td>
<td><code>cpcx CPC IPT LOG SPILL(n)</code></td>
<td>LOG SPILL (see page 267)</td>
</tr>
<tr>
<td>Activate IPT server trace output</td>
<td><code>cpcx CPC TRACE ACTIVE (Y)</code></td>
<td>TRACE ACTIVE (see page 266)</td>
</tr>
<tr>
<td>Deactivate IPT server trace output</td>
<td><code>cpcx CPC TRACE ACTIVE (N)</code></td>
<td>TRACE ACTIVE (see page 266)</td>
</tr>
</tbody>
</table>
IPT TRACE output

IPT server diagnostic tracing is not normally required.

It is controlled by the TRACE command in the cpcxINI file and the TRACE operator command. The IPT server address space uses this SYSOUT data set for messaging and diagnostic information. If the data set is not specified in the started task procedure, it is dynamically allocated.

TRACE ACTIVE

The following IPT server command activates IPTTRACE output (where cpcx is the BCSS/CPC subsystem identifier):

cpcx CPC IPT TRACE ACTIVE (Y)

The following IPT server command deactivates IPTTRACE output (where cpcx is the BCSS/CPC subsystem identifier):

cpcx CPC IPT TRACE ACTIVE (N)

TRACE SYSOUT

The following IPT server command writes all trace information to the specified SYSOUT class the next time that the IPTTRACE data set is allocated (where cpcx is the BCSS/CPC subsystem identifier):

cpcx CPC IPT TRACE SYSOUT(*)

Specify the SYSOUT class to be used the next time that the IPTTRACE data set is allocated.

TRACE SPILL

The following IPT server command writes all trace information to the IPTTRACE data set (where cpcx is the BCSS/CPC subsystem identifier):

cpcx CPC IPT TRACE SPILL(n)

Leave the SPILL specification blank to perform the spill immediately, or enter a number of lines following the SPILL function to override the SPILL keyword value in the CPCINI DD statement.

If you specify a number following the SPILL command, IPTTRACE is closed and reallocated after that number of records has been written to IPTTRACE. If no value is specified, the current IPTTRACE data set is closed and a new SYSOUT data set is opened. The specified number can be zero through \(10^{15}-1\). If you specify zero, the data set is never spilled.
IPTLOG output

The IPT server journal is controlled by the LOG command in the CPCINI file and LOG operator command. The IPT server address space uses this SYSOUT data set for messaging and diagnostic information. If the data set is not specified in the started task procedure, it is dynamically allocated.

LOG SYSOUT

The following IPT server command writes all log information to the specified SYSOUT class the next time that the IPTLOG data set is allocated (where cpcx is the BCSS/CPC subsystem identifier):

cpcx CPC IPT LOG SYSOUT(*)

Specify the SYSOUT class to be used the next time that the IPTLOG data set is allocated.

LOG SPILL

The following IPT server command writes all log information to the IPTLOG data set:

cpcx CPC IPT LOG SPILL(n)

Leave the SPILL specification blank to perform the spill immediately, or enter a number of lines following the SPILL function to override the SPILL keyword value in the CPCINI DD statement.

If you specify a number following the SPILL command, IPTLOG is closed and reallocated after that number of records has been written to IPTLOG. If no value is specified, the current IPTLOG data set is closed and a new SYSOUT data set is opened. The specified number can be zero through (10^{15}-1). If you specify zero, the data set is never spilled.

CPCINI keywords

This topic lists and describes the supported cpcxINI keywords.

The default cpcxINI sample member contains sufficient keywords for normal operations.

### cpcxINI keywords

<table>
<thead>
<tr>
<th>Command</th>
<th>Keyword</th>
<th>Required</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENV</td>
<td>NAME</td>
<td>Y</td>
<td>None</td>
<td>Specifies the logical name of environmental services to be initialized in the server address space. The name must be one to eight characters.</td>
</tr>
<tr>
<td>ENV</td>
<td>PARM</td>
<td>N</td>
<td>None</td>
<td>Eight-byte parameter field to be passed to environment services initialization module.</td>
</tr>
<tr>
<td>ENV</td>
<td>PROGRAM</td>
<td>Y</td>
<td>None</td>
<td>Identifies the program module to call to initialize the service.</td>
</tr>
<tr>
<td>Command</td>
<td>Keyword</td>
<td>Required</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The program module is also called for each function connecting to these services.</td>
</tr>
<tr>
<td>ID</td>
<td>DESC</td>
<td>N</td>
<td>None</td>
<td>Up to 50-character description used to identify CPC subsystem for user interface</td>
</tr>
<tr>
<td>LOG</td>
<td>SPILL</td>
<td>N</td>
<td>0</td>
<td>Number of lines to write to CPCLOG before automatically closing and reallocating new SYSOUT data set</td>
</tr>
<tr>
<td>LOG</td>
<td>SYSOUT</td>
<td>N</td>
<td>*</td>
<td>SYSOUT class to use for the CPCLOG data set</td>
</tr>
<tr>
<td>MIG</td>
<td>DATACLAS</td>
<td>N</td>
<td>None</td>
<td>Identifies the SMS data class of the unload file being allocated for migration</td>
</tr>
<tr>
<td>MIG</td>
<td>MGMTCLAS</td>
<td>N</td>
<td>None</td>
<td>Identifies the SMS management class of the unload file being allocated for migration</td>
</tr>
<tr>
<td>MIG</td>
<td>STORCLAS</td>
<td>N</td>
<td>None</td>
<td>Identifies the SMS storage class of the unload file being allocated for migration</td>
</tr>
<tr>
<td>MIG</td>
<td>THRESHEXT</td>
<td>N</td>
<td>200</td>
<td>Identifies the threshold value for maximum extents that is used during execution of the repository management EXPAND command. If you specify a value less than five, the original default value (200) is used. The maximum extents threshold used with the repository management EXPAND command is used exclusively as a repository management threshold. It is not related to the MAXM OSAM/VSAM Extents threshold defined in the console for user databases.</td>
</tr>
<tr>
<td>MIG</td>
<td>UNIT</td>
<td>N</td>
<td>None</td>
<td>Identifies the UNIT name of the unload file being allocated for migration</td>
</tr>
<tr>
<td>MIG</td>
<td>VOLS</td>
<td>N</td>
<td>None</td>
<td>Identifies the volume name of the unload file being allocated for migration</td>
</tr>
<tr>
<td>REP</td>
<td>PREFIX</td>
<td>N</td>
<td>None</td>
<td>26-byte prefix to use when allocating repository data sets You must change this name to accommodate your environment.</td>
</tr>
<tr>
<td>REP</td>
<td>RECS(p,s)</td>
<td>N</td>
<td>1000, 500</td>
<td>Default REC values (primary allocation, secondary allocation) to use when defining new repository data sets</td>
</tr>
<tr>
<td>REP</td>
<td>VOLS(vol,..., vol6)</td>
<td>N</td>
<td>None</td>
<td>Up to six default volumes to use when defining new repository data sets You must change this value to accommodate your environment.</td>
</tr>
<tr>
<td>START</td>
<td>MODE</td>
<td>Y</td>
<td>None</td>
<td>MODE specifies that the server is private.</td>
</tr>
<tr>
<td>START</td>
<td>NAME</td>
<td>Y</td>
<td>None</td>
<td>NAME(ALL) is used for all product functions NAME(CPCSAMP) is used for all CPC sample functions. Any function can be started by operator command.</td>
</tr>
<tr>
<td>START</td>
<td>TYPE</td>
<td>Y</td>
<td>None</td>
<td>TYPE(FUNCTION) is used to specify which functions are started at CPC initialization. TYPE(COM) is used to start the Comm Server in this address space.</td>
</tr>
<tr>
<td>TRACE</td>
<td>ACTIVE</td>
<td>N</td>
<td>N</td>
<td>Identifies whether tracing is to be started when the server address space is initialized</td>
</tr>
<tr>
<td>XSYS</td>
<td>GROUP</td>
<td>Y</td>
<td>None</td>
<td>One to eight-character cross-system group name; must be a unique XCF group within the SYSPLEX All cpxctNI keywords must point to the same XSYS(GROUP) name.</td>
</tr>
<tr>
<td>Command</td>
<td>Keyword</td>
<td>Required</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>XSYS</td>
<td>MASTER</td>
<td>N</td>
<td>None</td>
<td>Defines the MVS image on which the IPT server master resides. For more information about how the master IPT server works, see Sysplex implementation (see page 264).</td>
</tr>
<tr>
<td>TRACE</td>
<td>SPILL</td>
<td>N</td>
<td>0</td>
<td>Number of lines to write to CPCTRACE before automatically closing and reallocating new SYSOUT data set.</td>
</tr>
<tr>
<td>TRACE</td>
<td>SYSOUT</td>
<td>N</td>
<td>*</td>
<td>SYSOUT class to use for the CPCTRACE data set.</td>
</tr>
<tr>
<td>XSYS</td>
<td>THREADS</td>
<td>N</td>
<td>1</td>
<td>Number of pipes to use per remote host.</td>
</tr>
<tr>
<td>A</td>
<td>SYSPLEX</td>
<td>A</td>
<td></td>
<td>Specify whether to use XIM.</td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any valid unit name</td>
<td>XIMDASD</td>
<td>SYSDA</td>
<td>Assign a unit name for SYSPLEX DASD.</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>SYSPLEX</td>
<td>A</td>
<td></td>
<td>Specify whether to use XIM.</td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any valid unit name</td>
<td>XIMDASD</td>
<td>SYSDA</td>
<td>Assign a unit name for SYSPLEX DASD.</td>
<td></td>
</tr>
</tbody>
</table>

You must specify the CPCINI control statement data set in the IPT started task procedure (cpcx IPT). The control statement must contain 80-character fixed-length records. A command can have keywords and comments. Separators and continuation characters are supported. You can enter commands anywhere in positions 1 through 72 of the input statement (positions 73 through 80 are ignored). See the CPCINI sample member in the sample library for your solution or product.
Index

a

acbgen 20
access 31
accessing bmc uim server commands web page 235
activate tracing 266
activating 190
activating tracing for the ipt server 266
active 267
active keyword 267
add 20, 31
add bmclink 20
add ims to group log 107
add ims to group log panel 107
adding user access authorization 31
add user access authorization 31
administrator authority 60, 147
after initial installation 164
agn 42
allocate new data set type 104
allocate new data set type panel 104
allocating 247
allocating hfs 247
allow ims storage displays 42
allow ims storage zaps 42
allowing 164
allowing use of 164
allow netcmd 235, 244
alternate imsid 42, 75, 156
altview 92
altview primary command 92
apf authorization 261
appc 42
mvs data set name 42
applctn 20
asm source member 173, 185
assemble and link edit the mode table 202, 204
associated db 30, 59, 145
dc functions 30, 59, 145
associated delta plex functions 67
auid 173, 185
auid macro 173, 185
authentication 229
auth timeout secs 244

b
base imsid options 42
base imsid options panel 42
bcss 261, 262
cpc subsystem 261, 262
bmclink 20
bmclink command authorization 20
bmclink enq qname 37
bmclink enq rname 37
bmcnodecntl 173, 185, 190, 193, 212
bmcnodesamp 173, 185, 202, 204
bmcp 258, 260
bmcp subsystem 259, 259
bmc system administration for ims 14
bmc system communication for ims 11, 17
bmc uim server commands web page 235
browser 228

C
cancel 91
cancel primary command 91
change 20
changing 238
check 37
execute pacing value 37
check delta list 37
checkpoint dsn 190
clear 92, 92
clear primary command 92, 92
client 228
command defaults 92
commands 92, 259, 262
comment 92
configuration 90
configuration worksheet 53
confirm add ims pop up window 107
connecting 232
connection 231, 232
console 227, 228, 229, 229, 229
copy 91
copy options to the ims reslib 42
copy primary command 91
cpc start adv 243
cpc start ipt 243
cpcxadv 243
cpu id options 87
creating 90
creating elinks 132
creating new 90
cross domain access 204
customization 37, 83, 153, 162
customization worksheet 11, 14, 17, 20, 53, 127, 129, 139, 166, 179, 227
data sets 247
dbctl 42
dbctl control region indicator 42
default 91
default primary command 91
defaults 170
default value 92
defhs member 247
defining 232
delta ims db 20
dc 20
delta ims dc 20
delta ims for dbctl 20
delta ims virtual terminal 20
delta plex data set allocation menu 104
delta plus 53
delta plus virtual terminal 127
delta plus virtual terminal imsid options 112, 114, 116
desc 267
desc keyword 267
description 92
dfspbxxx 164
displaying the status of the bcss 262
cpc subsystem 262
displaying the status of the bmcp subsystem 259
display status 259, 262
dlasau0 27
dlatss 27
dlaxalb0 27
dlaxctl0 20
dlaxts0 27

edit 91
edit global options 71, 153
edit global options panel 71, 153
edit group options 83, 162
edit group options panel 83, 162
edit primary command 91
element access 92
element type 92
elinks 132
enable delta plus virtual terminal 114
enable ims connect authentication 133
enable transaction authentication 133
enable userid authentication 133
energizer appl statements 134
energizer for ims connect 129
energizer ispf interface 133
enterprise list 231, 232
env 267
env command 267
establishing administrator authority 60, 147
establishing through racf 60, 147
etaiili modules 164
etaxrcn0 60, 147
execute delta list 37
execute started tasks 262
exiting 229
extended terminal assist plus 139
extract 190
extract data set 190
extract dsn 190

f
field access 92
field id 92
field name 92
field order 92
force update when queue count 92
0 92
for group option module instructions for specifying 83, 162
for imsid option module instructions for specifying 71, 75, 109, 153, 156, 160
format the logs 42

generic dasd unit name 37
global 37, 153
global options 37, 153, 162
global options entry 71, 153
global options entry panel 71, 153
global options library 162
global options panel part 1 37
global options panel part 2 37
global options part 1 37
global options part 2 37
group 83, 162, 267
group keyword 267
group options 83, 162
group options library 162
guidelines 24, 54, 141
guidelines for creating 24, 54, 141

h
hfs dataset 244
hfs directory 252
history information 37
id 267
id command 267
idle bmp automatic shutdown interval 37
implementing 70
ims appl statements 141
ims appl statements for session manager true nodename support 141
ims connect resource 133
ims control region jcl 164
imsid 75, 83, 109, 156, 162
group options entry 75, 109, 156
group options entry panel 75, 109, 156
imsid options 42, 75, 156, 162
imsid options library 160
imsid options panel 42
imsid options update enq qname 37
ims operator commands 37
ims proclib data set 42
ims proclib data set for dbctl 42
ims proclib member 20
ims reslib data set name 42
ims version 42
release level 42
initializing 247
initializing hfs 247
installation 228
installation procedure 210
installation verification procedure 213
installing 228
installing console 228
instructions for creating 24, 54, 90, 141
instructions for specifying 71, 75, 83, 109, 153, 156, 160, 162
instructions for use 60, 147
internal eta security 60, 147
internal trace table dynamic dump sysout class 37
internal trace table size 37
iprcpum 136
iprjrna 134
ipropts 134
ipt 267
iptlog output 267
ipt server 262, 264, 264, 265, 266, 266, 266, 266, 267, 267, 267
ipttrace output 266
ispf 57, 130, 144, 167, 181
pdf primary option menu 57, 130, 144, 167, 181
ispf interface 132
ispf profile defaults 168

j
jcl requirements 262

k
keywords 267

l
launching 229
lcpps01 170
lcpxsma0 173
libdef service 27
libraries 190, 193, 202, 212
library 71, 75, 83, 109, 153, 156, 160, 162
local copy plus 166
log 267
log command 267
logical unit names 24, 54, 141
log ims operator commands 42
log output 267
luname 134

m
macro 92
macro off 92
macro off primary command 92
macro on 92
macro on primary command 92
maintenance 234, 258
managing 232
marked for execution 92
masking 219
master 267
maximum dl 37
i command size 37
message advisor checkpoint tracking 190
message advisor checkpoint tracking data set 190
message advisor for ims 179
mode 267
mode keyword 267
mode table 24, 54, 141
modifications to 27, 57, 130, 144, 167, 181
modules 27
multiple signons per user id 164

n
name 267
name keyword 267
normal member 249

o
open 91
open primary command 91
operating 255
operating uim server 255
operator 37
options 162
override imsid 42
overview 228, 259, 260

p
panel defaults 28
panel for specifying 71, 83, 153, 162
panels 42, 71, 75, 96, 104, 107, 109, 156, 162, 183
parm 267
parm keyword 267
password 133
perform an ims psbgen and acbgen 20
personal list 231
port 244
prefix 267
prefix for bmclink session acbname 24, 37, 54, 141
prefix keyword 267
primary and secondary logs 42
primary commands 91, 91, 92, 92
proclib member dfspbxxx 164
profile defaults 28
program 267
program keyword 267
program name dlaxctl0 20
prompt 92
prompt primary command 92
psbgen 20
psb name 42

q
qmrallo 190
qmrappl 201
qmrivp1 214
qmrsm0 173, 185
qmrstrt 212
qmrxml0 173, 185
qmrxmlsma0 185
qname 37
qpf test applications 210

r
racf 59, 60, 147
rcf parameter ims 164
recs 267
recs keyword 267
refreshing 87, 126
refreshing content 239
refresh menu 75
remarks 92
rep 267
rep command 267
repository 234, 258
repository maintenance 234
request library create 183
request library create panel 183
request status check time interval 37
required parameters in jcl 164
rmgr 258
rname 37
rprefixconnres 133
rprefix dis 133
rprefix exec 133
rprefix rel 133
rprefix res 133
rprefix set 133

S
sample 24, 54, 141
sample cdrsc statements 24, 54, 141
sample library 240
samples 24, 54, 141
sample statements 134
save 91
save library 162
save primary command 91
scrap 190
scrap data set 190
scrap dsn 190
security 20, 70, 133, 264
select field for revise 92
selecting options 42
session manager true nodename support 141
setting limits 112
setting limits for virtual terminals 112
sgn parameter ims 164
smu 20, 164
specify trancmd 20
spill 267
spill1 190
spill1 dsn 190
spill2 190
spill2 dsn 190
spill3 190
spill3 dsn 190
trace command 267
trace output 266
tracing options 238, 238
trancmd 20
transact 20
transaction code 42
trclogdd 238, 238
troubleshooting 238, 238
tso 24, 28, 54, 141
ispf 28
ispf appl statements 24, 54, 141
tso acbnames 24, 54, 141
tso lu names 24, 54, 141
tss tables 126
type 267
type keyword 267

U
uim 240
uim member 245
uim server 228, 234, 235, 237, 239, 244, 245, 249, 252, 255
uim server appl statements 134
uimx member 240
uninstallation 229
uninstalling 229
unload 190
unload data set 190
unload dsn 190
unsolicited output transact table name 116
update 229
update smu 20
update user access profiles 31
update user access profiles panel 31
updating 164
updating in the control region 75, 83
user authorization exit name 42
user customization exit name 42
user id 59
user id for authorization check 37
user interface middleware uim server 228
user profiles data set name 37
user profile sort 31
user profile sort panel 31
using with ispf 201

V
valid dynamic transaction names 116
verifying module storage 164
verifying storage of 164
viewing active users 237
view profile edit 96
view profile edit entry 96
view profile edit entry panel 96
view profile edit panel 96
view profile element edit 96
view profile element edit panel 96
view profile field edit 96
view profile field edit panel 96
view profile name field 92
view profiles 90
vols 267
vols keyword 267
vtam , , , , 24 54 134 141 204
vtam definitions , , 24 54 141
vtam lu 62 session 201
vtam statements 134

W
with message advisor auto req cmd 193
with message advisor data set names 193
write log information 267
write tracing information 266
writing log information for the ipt server 267
writing tracing information for the ipt server 266
wto message descriptor codes 37
wto message routing codes 37

X
xrf alternate ims apf authorized library 42
xrf alternate imsid 42
xsys 267
xsys command 267

Z
z 229
os 229
os authentication 229
The information included in this documentation is the proprietary and confidential information of BMC Software, Inc., its affiliates, or licensors. Your use of this information is subject to the terms and conditions of the applicable End User License agreement for the product and to the proprietary and restricted rights notices included in the product documentation.

BMC Software Confidential.

The information included in this documentation is the proprietary and confidential information of BMC Software, Inc., its affiliates, or licensors. Your use of this information is subject to the terms and conditions of the applicable End User License agreement for the product and to the proprietary and restricted rights notices included in the product documentation.

Click here for the provisions described in the BMC License Agreement and Order related to third party products or technologies included in the BMC product.

BMC Software, Inc.
2103 CityWest Blvd, Houston TX 77042-2828, USA
713 918 8800
Customer Support: 800 537 1813 (United States and Canada) or contact your local support center